EISOO AnyBackup Appliance 5.0
— User Manual

Copyright

About EISOO

Being one of the fastest-growing suppliers of All-in-One solutions for backup, storage and disaster recovery, EISOO continually exceeds expectations in the areas of innovation, professionalism and sincerity when researching and developing products, aiming to satisfy the needs of customers and make information more effective.

Through continuing development, EISOO has gained experience in data protection, network storage and business continuity by releasing a series of highly cost-effective solutions and services which include the widely-used EISOO AnyBackup Family, powerful EISOO T×3 Cloud Platform and EISOO AnyShare which is an All-in-One device for file management. Thus it has enabled hundreds of thousands of users to experience the amazing features of data protection and business continuity, with clients including governments, enterprise, electric power, education, health care, research institutions and more.

It is EISOO's ceaseless innovation that leads users' needs, helping to ensure data security and enhancing business value under such high-speed development.

Contact Us

Address: 2nd floor, No. 8 Building, Pujiang Intelligence Valley, No. 1188 Lianhang Rd, Minhang District, Shanghai, China
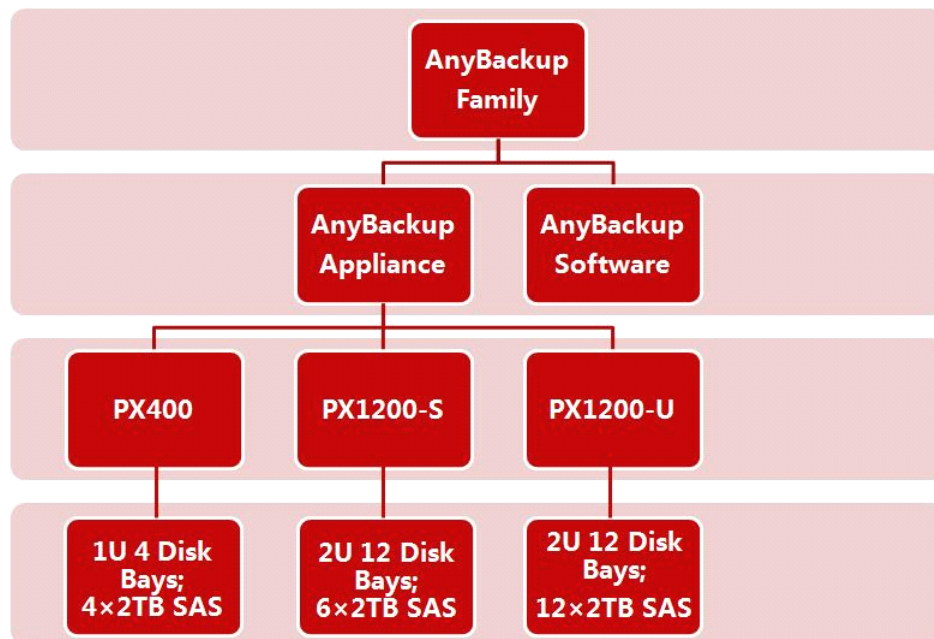
Zip Code: 201112

Tel: 021-54222601

Email: support@eisoo.com

Web: www.eisoo.com/en

EISOO AnyBackup Family

Adhering to "All-in-One Protection", EISOO released AnyBackup Family 5.0 which covers both software and hardware products, namely AnyBackup Software 5.0 and AnyBackup Appliance 5.0. AnyBackup Appliance 5.0 can be further divided into PX400, PX1200-S and PX1200-U.

```
                    ┌─────────────┐
                    │  AnyBackup  │
                    │   Family    │
                    └─────────────┘
              ┌─────────────┐  ┌─────────────┐
              │  AnyBackup  │  │  AnyBackup  │
              │  Appliance  │  │  Software   │
              └─────────────┘  └─────────────┘
      ┌──────────┐  ┌──────────┐  ┌──────────┐
      │  PX400   │  │ PX1200-S │  │ PX1200-U │
      └──────────┘  └──────────┘  └──────────┘
    ┌───────────┐  ┌───────────┐  ┌───────────┐
    │ 1U 4 Disk │  │ 2U 12 Disk│  │ 2U 12 Disk│
    │   Bays;   │  │   Bays;   │  │   Bays;   │
    │ 4×2TB SAS │  │ 6×2TB SAS │  │ 12×2TB SAS│
    └───────────┘  └───────────┘  └───────────┘
```

CONTENT

Preface

Thank you for choosing EISOO AnyBackup Appliance 5.0. To avoid unintended device damage, please read this document carefully before installing and using it. If you have any problem, please do not hesitate to contact us.

This document is for:

- ◆ Network Engineers
- ◆ Network Administrators
- ◆ Anyone who is interested in our products

Chapter 1 Overview

1.1 About AnyBackup Appliance 5.0

As a leading All-in-One device, EISOO AnyBackup Appliance 5.0 is designed to provide users with innovative solutions. It can satisfy centralized backup for PC and server environment which includes Windows, Linux and Unix. This device also adopts a combination of multiple storage structures of NAS, IP SAN and FC SAN to satisfy the needs of data sharing and centralized storage.

1.2 Basic Modules and Their Functions

EISOO AnyBackup Appliance is composed of the following modules:
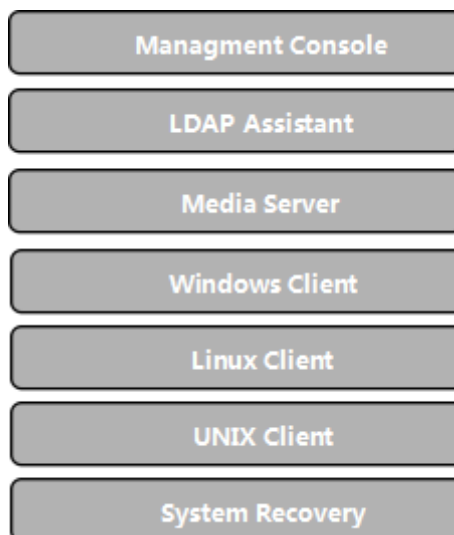
1.2.1 Management Console (Console)

Management console provides a browser-based operation interface and a storage server. It allows the system admin to centrally allocate user and storage space, install/manage/configure remote client, configure replication job, manage virtualization platform, configure full copy count of backup set, create data backup and restore and view schedule/status/logs of all backup jobs.

Management console allows different users to manage user, data, client and perform data backup and restore based on authorization. User can be divided into [Admin] and [Ordinary User], both can enter the web interface of the management console (e.g. http://192.168.1.110:9800) by entering the account name and

password, selecting language and clicking [Login]. "192.168.1.110" is the IP address of the console and "9800" is the default port.

Admin can create user, allocate backup space, specify storage path, view backup schedule/status/log, create and manage backup data and restore data on the terminal machine on which the browser is installed at any time and any place you want.

Ordinary user can view own job schedule, storage space status, backup log and create/manage data, restore data and more.

Via management console, all file, email, system, database and VM on local and remote client can be backed up and data can be directly restored to a specified client. Detailed functions are:

➤ Support for incremental backup for various kinds of files, which backs up modified or newly-added files only, so as to enhance backup speed and save storage space.
➤ Support for incremental backup and restore for mails of Outlook, Outlook Express, Foxmail, Thunderbird, Windows mail, Windows Live mail and more.
➤ Support for incremental backup of operating system without halting and instant system restore when system fails due to hardware failure, virus and more.
➤ Support for full, differential and transaction log backup for Microsoft SQL Server database log and file group.
➤ Support for full, incremental and transaction log backup for Oracle database; support for backup and restore of the whole instance.
➤ Support for full, incremental backup and restore for Sybase.
➤ Support for backup and restore of Active Directory database, transaction log file and checkpoint file.
➤ Support for full and incremental backup and restore for data in Lotus Domino database.
➤ Support for full, incremental backup of Exchange Server database, support for backup and restore of storage group (Exchange Server 2003/2007) and database (Exchange Server 2010).
➤ Support for full, incremental and differential backup of DB2 database.
➤ Support for full backup and restore of MySQL database.
➤ Built in VMware Server platform, which supports rich VM management system and VMware backup and restore.

- ➢ Support for full, incremental backup and restore of Hyper-V platform.
- ➢ Schedule, auto backup can be configured for backup jobs.
- ➢ Support for backup rotation, max full backup copy count can be set.
- ➢ Support for data compression and encryption when backing up.
- ➢ Support for flow control during backup.

Management console also provides centralized backup, restore and execution management and more. Detailed features are:

- ➢ Based on B/S structure, admin can access to management console remotely on any computer to achieve unified management.
- ➢ Backup management, used to centrally set backup schedule and create backup jobs to execute data backup for clients.
- ➢ Restore management, admin or users can restore backup data to specified client via management console.
- ➢ Execution management, used to display status or progress of backup and restore and history of each execution.
- ➢ Log management, admin or user can check related logs generated in using AnyBackup Appliance.
- ➢ User management, admin can create user account, modify user info and bind user client and storage media.
- ➢ Client management, used to configure, group, delete client and more.
- ➢ Dual-HA/Cluster management, used to achieve Dual-HA/Cluster client binding, configuration, binding deletion and more.
- ➢ Disk media management, admin can centrally manage all media and media servers, and manage storage media and device.
- ➢ Media sync management, used to create, modify and delete media sync job.
- ➢ License management, used to manage permissions.
- ➢ System configuration, used to configure management console with specific conditions.
- ➢ Warning configuration, used to send message to system admin by configuring email, sound or email warning function.
- ➢ Update management, used for manual or online update.
- ➢ Self backup management, used for self backup and restore for management console itself.
- ➢ Report management, provide reports of console security, business status to system admin or different sites in the form of multi-graph, so as to help understand info of system security, job execution, data security, data storage

and more., thus performing effective management for system risk.

1.2.2 LDAP Assistant

LDAP assistant is to separate console and domain user function. It adds domain user function to a sole service program and provide sole installation package to install id authentication agent. LDAP assistant will search for the console automatically and connect to it for data transfer.

➢ LDAP assistant allows connection to multiple consoles, but one console can connect with only one LDAP assistant. The existed connection will be cleared if a new connection is made.

➢ To avoid unauthorized adding, console admin password needs to be verified when adding LDAP assistant to console.

➢ Connected console can be deleted via LDAP assistant. Enter admin password to finish deletion.

➢ A "Fail to connect" alert will display if LDAP assistant is not connected normally.

1.2.3 Media Server

If you need to store data on another storage device, you can install media server agent. To differ from master media server which is configured when installing and configuring console, it is referred to as a sub media server. It is installed on Windows or Linux platform, used to accept the management control of console, respond to backup and restore scheduling and accept backup data from client.

➢ Provide media binding, support serial connection of multiple physical or logical media devices to constitute more storages

➢ Provide quota management of media space, which limits max media space for authorized user

➢ To accept backup data from client and store to specified media

➢ To accept the restore request of client or console and restore data to specified client

1.2.4 Windows Client

Windows client is used for systems above Windows 2003. It is deployed on the server or PCs to be backed up to respond to commands from console and provide backup and restore functions for file, OS, mail, database and VM.

➢ Normal Client

Normal client is usually installed on computers of ordinary staff, all data can be viewed and operated by admin. It contains the Client engine which can be accessed by console at any time, used to show backup status and restore components integrated by system Explorer. It also enables restoration of files in Explorer

whenever required.

➢ Daemon Client

Daemon client is usually installed on computers of ordinary staff, all data can be viewed and operated by admin. It is used for forced backup. Besides the Client engine, it has no interface and cannot be uninstalled directly on the client. Password provided by admin is needed when uninstalling.

➢ Secure Client

Secure client is usually installed on the computer which stores sensitive data, one user is bound and only this user can check and operate data on this computer (even the admin is unable in this state). The only difference from the Normal Client is that it binds a user.

1.2.5 Linux Client

Linux client is deployed on Linux system to protect data on Linux platform. It is used to respond to console commands. Current Linux client supports daemon client only and needs to start AnyBackupClient process manually to respond to console request.

1.2.6 Unix Client

Unix client is deployed on Unix system to protect data on Unix platform. It is used to respond to console commands. Current Unix client includes AIX, HP-UX and Solaris.

1.2.7 System Recovery Environment (SRE)

SRE is an indispensable component in system backup and is used for system restore.

➢ Support for system restore of PC and server

➢ Support for connecting to media server to find system backup set and to restore to client

➢ System restore user can be bound for auto connection to media server for restore

➢ Greatly reduce computer maintenance time if combined with bare metal restore

Chapter 2 Introduction

2.1 Deployment

2.1.1 Security Statement

◆ **Be careful**

To avoid electric shock, please do not open. No internal parts are user serviceable. Please contact your distributor for service and warranty information.

◆ **Introduction**

Before installing and operating AnyBackup Appliance, please read this manual carefully. For later reference, please reserve this manual.

Please do not try to repair this product by yourself, as it may cause damage, which will void the warranty.

◆ **Statement**

This is a level A product which follows the GB9254-2008 standard. In a living environment, it may cause radio interference, so measures may be necessary to reduce this.

Note: living environment may refer to broadcast or television receiver used 10 miles away from this device.

◆ ⚡**Warning**

Please ensure the rack or desktop to put AnyBackup Appliance can bear the server. Please avoid strenuous vibration during operation as it may lead to physical damage.

2.1.2 Important Notice

The RAID technology in AnyBackup Appliance can make data more reliable and securer, but not absolutely. An unsuitable physical environment, vibration, misuse or disk failure is likely to cause device damage and data loss. Thus, please do re-backup for critical data to prevent fatal loss. Furthermore, please pay attention to the running status of the device. If there are warnings such as sound, light and email, or when a disk fails, please contact us as soon as possible.

2.1.3 Working Environment

AnyBackup Appliance works within the temperature and humidity range as shown in the following table. Sufficient air circulation is also needed.

Environment	Range
Operating Temperature	0℃~40℃ (32℉~104℉)
Operating Humidity	10%~85%

Figure 1 Table of working environment

AnyBackup Appliance works under certain power environment as shown in the following table:

Environment	Range
Operating Voltage	200VAC ~ 240VAC or 100VAC ~ 125VAC
Operating Current	<3.5A or <7A
Operating Current Frequency	47Hz ~ 55Hz

Figure 2 Table of power environment

✗Warning: AnyBackup Appliance must work under the above environment; otherwise, physical damage may be caused.

2.2 Hardware Installation

2.2.1 Device Electrification

Insert one end of power line to the power input slot of the AnyBackup Appliance and the other to the power socket or the output slot of UPS, as shown in the following figure:

Figure 3 Power connection

2.2.2 Network Connection

Insert one end of Ethernet cable to the Ethernet port of server and the other to HUB or Switch port.
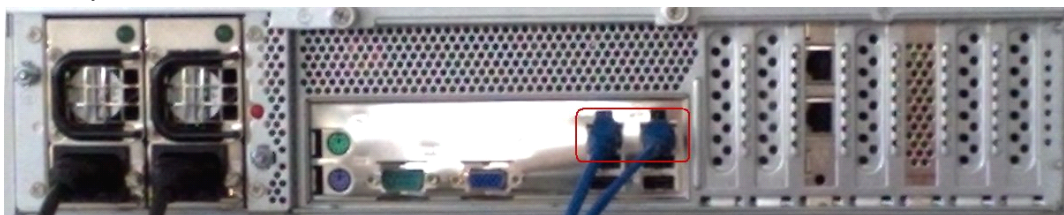

Figure 4 Network Cable

⚡Warning: Please ensure the power switch on the front panel is off when connecting power cable; otherwise, device will be damaged.

2.2.3 Disk Installation

If you want to install or replace disk, you can pull out the disk tray and install as shown below then tighten the screw.

Figure 5 Insert/pull out disk

2.3 Start and Shutdown

◆ **Start System**

Make sure the power line is connected to the power slot on the back of AnyBackup Appliance and the Samsung-grounded power socket.
Press the switch on the front panel and start AnyBackup Appliance.

◆ **Restart System**

AnyBackup Appliance provides two ways to restart system:

➢ **Restart Normally:** you must log in to the Web console and click [Restart Device].

➢ **Forced Restart:** press the pinhole above the restart icon with a needle-like object within 5 seconds and system will restart. Its symbol is " ↻ ".

◆ **Shutdown System**

AnyBackup Appliance provides two ways to shutdown system:

➢ **Shutdown Normally:** you must log in to the Web console and click [Shutdown Device]. The whole shutdown takes 30 seconds or so and the power light will switch off.

➢ **Forced Shutdown:** If the power button is pressed for 5 seconds when system is running, an abnormal shutdown program will be started and system will be switched off. When the system restarts, it will perform an automatic check and restore.

ⓘ**Caution:** data loss will be caused and the next service entering will be postponed if forced shutdown is used. Please try to avoid it.

2.4 Login

Three login ways are provided by AnyBackup Appliance, namely Based on Password, Based on USB-Key, and Based on Password and USB-Key.

2.4.1 Login Mode

Enter the login interface of the console via such links as http://192.168.1.110：9800 (default address of console), just as the following figure shows:
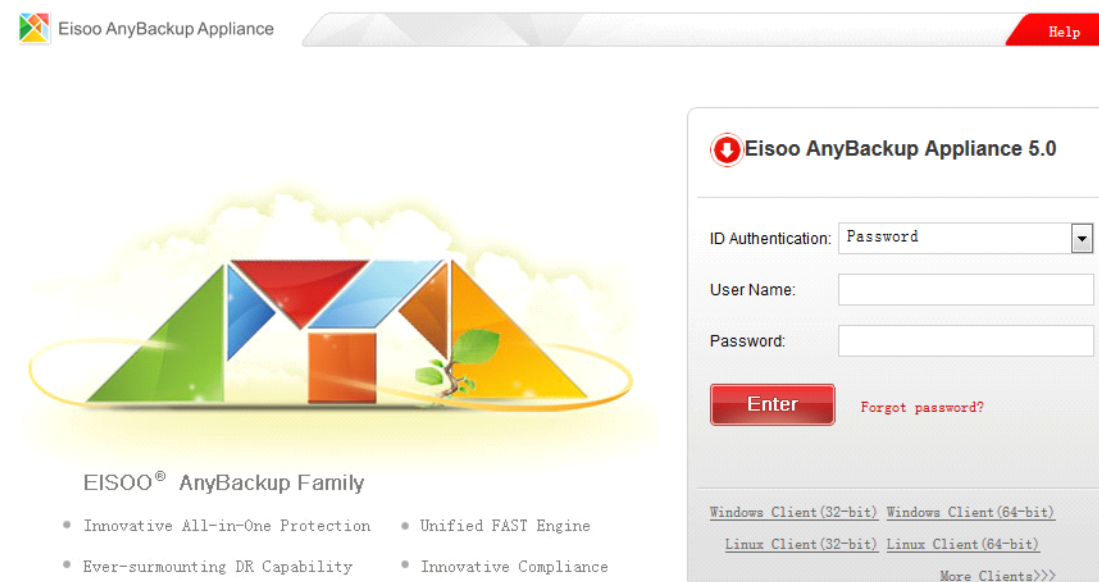
Figure 6 Login interface

Select the authentication mode to log in to the management console:

◆ **Based on Password**

➢ Admin account has been pre-set by AnyBackup Appliance with the username as "admin" and initial password as "123456".

➢ After logging in, the admin can create user in [Configuration] >> [User] >> [New].

➢ When a user logs in, enter the username with initial password of "123456".

➢ If audit admin is enabled, log in with username "audit" with initial password of "123456".

◆ **Based on USB-Key**

Only one user is bound to one USB-Key. Insert the USB-Key and use Internet Explorer to download and install the plug-in.

◆ **Based on Password and USB-Key**

Data security is ensured more effectively. Insert the USB-Key and select [Based on Password and USB-Key] in [ID Authentication] and enter the username and password bound with the USB-Key. Click [Login] to log in the management console.

2.4.2 First Login

When logging in to the console for the first time, a dialog box with "Password and Email Bound" will display for admin to modify the password and configure the email that is bound.

[Configure Email Notification] is used to set the SMTP email address (e.g. smtp.eisoo.com), port (25 by default), username (email address of addresser) and password (email password). After configuration, you can select [Send Test Email] , and enter addressee email in the box labeled [Please enter email address]. You can check if test email is sent successfully. If you have received this email, it demonstrates that your email notification function is configured correctly.

After configuration, please check the top right corner of the page. You should find the following options: User, Modify Password, Modify Email, Email Notification, Help and Exit.

[Modify Password]: modify the login password of users.

[Modify Email]: modify the email address of email notification.

[Email Notification]: two kinds of notification types are provided, that is, notify when backup succeeded and notify when backup failed.

[Help]: read documentation on operation of AnyBackup Appliance.

[Exit]: return to the login page.

Chapter 3 Device Configuration

Before installation and usage, you need to understand the system requirements of each function module and perform configuration, such as default login account, client, and more.

3.1 LDAP Assistant

LDAP assistant can be deployed on Windows domain controller to realize seamless support for ID authentication based on Windows domain controller.

3.1.1 System Requirements

Item	Requirements (required)	Requirements (recommended)
CPU	900 MHz	1.2 GHz or above
Memory	512 MB	1 GB or above
Disk Space	5 GB	20 GB
OS	Windows XP or later	Windows Server 2003

Figure 15 System requirements of LDAP assistant

3.1.2 Installation Wizard

LDAP can be installed by using the installation package as follows:

Step 1: Enter Windows system of client on which LDAP assistant will be installed, and start the AnyBackup Appliance installation program, select the default language to enter the start page.

Step 2: Click "Auxiliary Module", select [LDAP Assistant] and click [Install].

Step 3: Enter "Installation Program-EISOO AnyBackup Appliance LDAP Assistant" and click [Next]. Read "EISOO End User License" and select [I agree]. Then click [Next] to continue.

Step 4: Click [Browse] to select the installation path. Click [Next] and [Install] to start installation.

Step 5: After installation, click [Done].

3.1.3 Configuration

After installation of LDAP assistant, click [Start] >> [All Programs] >> [EISOO AnyBackup Appliance 5.0] >> [LDAP Assistant] >> [LDAP Assistant Configuration]

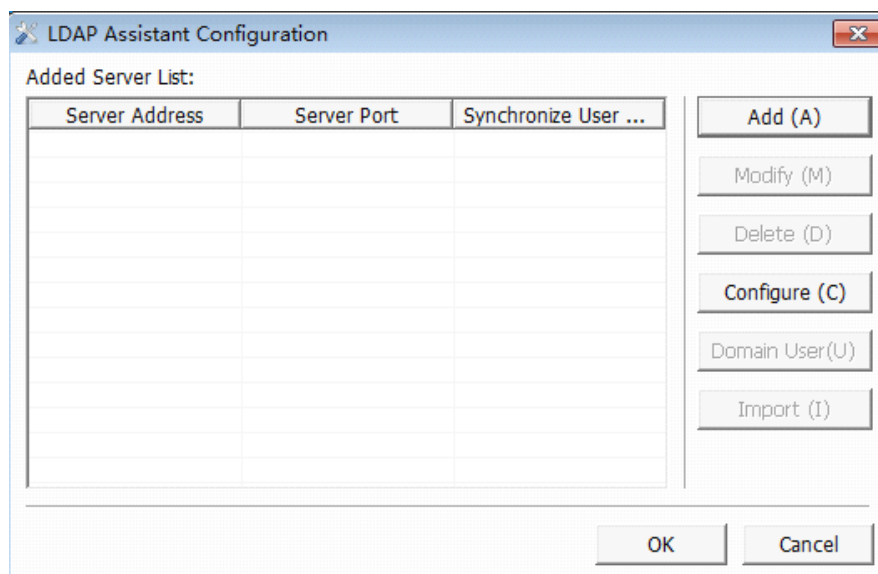to displaya dialog box for configuration. LDAP assistant can connect to multiple management consoles.

Figure 16 Configuration Interface

Click [Add] to show the configuration window. Enter the server address and admin password (default port is "9900" and the admin account is "admin").

Figure 17 Add Server

3.1.4 Uninstallation
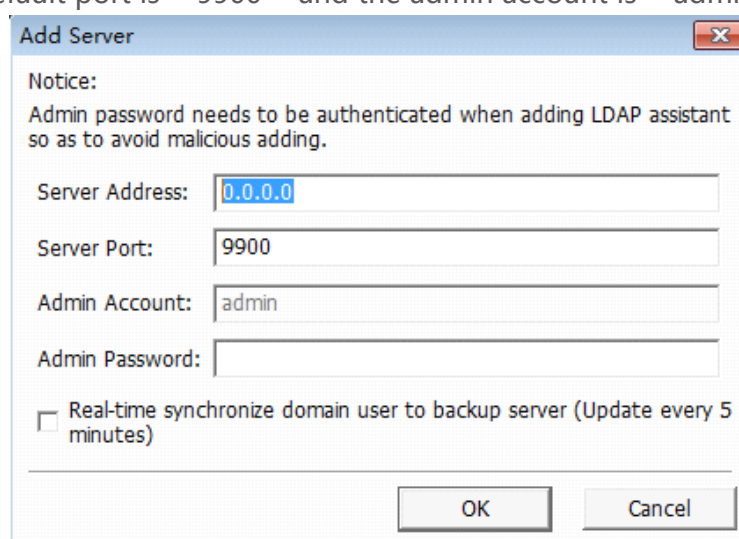
◆ **[Via System]**

Click [Start/Control Panel/Add or Remove Program] in the Windows desktop and select [LDAP Assistant]. Click [Uninstall] to uninstall LDAP assistant.

◆ **[Via AnyBackup Appliance]**

Select [Start/All Programs/EISOO AnyBackup Appliance 5.0/LDAP Assistant] in Windows desktop and click [Uninstall LDAP Assistant]. Click [Yes] when prompted to confirm uninstallation.

3.2 Windows Client

The client agent is deployed on the server or PC to be backed up. It responds to the command of console, providing data for users to back up and restore.

Client can be installed by starting the installation program on the local Windows system or downloading through the console interface. There are three kinds of Windows clients:

➢ Normal Client: Usually installed on computers of ordinary staff, all data can be viewed and managed by the administrator. It contains a client engine which can be accessed by console at any time and a display page to show basic client information.

➢ Daemon Client: Usually installed on computers of ordinary staff, all data can be viewed and managed by the administrator and can be used for forced backup. Besides the client engine, it has no interface and a password is required when uninstalling.

➢ Secure Client: Usually installed on computers which store sensitive data. One user is bound and only this user can check and manage data on this computer (even the administrator has no access). The only difference from the Normal Client is that it binds a single user.

3.2.1 System Requirements

Item	Requirements (required)	Requirements (recommended)
CPU	900 MHz	1.2 GHz or above
Memory	512 MB	1 GB or above
Disk Space	5 GB	20 GB
OS	Windows Server 2003 or later/ Windows XP (64bit) or later	Windows Server 2003 or later /Windows Server 2008 (64bit)

Figure 18 System requirements for Windows client

3.2.2 Normal Client

◆ **Installation**

Step 1: In Windows, start the AnyBackup Appliance installation program. Select the language and click [Next] to continue.

Step 2: Click "Install Client" in "Installation Program-Initial Page" to enter

[Installation Program-Select Modules] and select [Backup Client]. Click [Install].

Step 3: Start decompressing the installation package, and the client installation wizard will display after it finishes. Click [Next] to read "License" and select [I agree]. Click [Next] to continue.

Step 4: Select client type: Normal Client and click [Next] to continue.

Step 5: The program will be installed to C：\program files\Eisoo AnyBackup Appliance\5.0 Client\ by default. Click [Browse] to change the installation directory and then click [Next] to continue.

Step 6: In the [Backup Server] page, you need to set the IP address of the backup sever where the management console is installed, thus client info can be written to the management console automatically. If [Use default server address] is selected, the default IP and port: 127.0.0.1:9900 will be adopted. Click [Next] to continue.

Step 7: In the [Client Service] page, you need to select a username for the client service, which will decide local resource that the client can access to.

Step 8: Click [Install] to start client installation to specified user.

◆ **Uninstallation**

There are two ways to uninstall the Windows client of AnyBackup Appliance:

➢ **[Via System]**

Click [Start/Control Panel/Add or Remove Programs] from the Windows desktop, select [EISOO AnyBackup Appliance 5.0 Client] and click [Delete]. Then click [OK] in the confirmation window to delete the Windows client.

➢ **[Via AnyBackup Appliance]**

Select [Start/All Programs/EISOO AnyBackup Appliance 5.0 Client/Uninstall Client] and click [OK] in the confirmation window to perform uninstallation.

3.2.3 Secure Client

◆ **Install**

The installation of the Secure Client is almost the same as that of the Normal Client, please select [Secure Client] when selecting client type.

◆ **Configure**

Log in to the management console after successful installation and bind one user to it. Then log in with this user and activate the Secure Client on [ID Authentication of Secure Client] by entering the username and password of the machine where the secure client is installed. Click [OK] and the bind is complete. Or you can click

[Cancel] to go back to the homepage.

◆ **Uninstall**

The uninstallation of the Secure Client is almost the same as that of the Normal Client.

3.2.4 Daemon Client

◆ **Install**

The installation of the Daemon Client is almost the same as that of the Normal Client, but select [Daemon Client] when selecting client type.

◆ **Configure**

Daemon client is a forced client, which can be operated by management console only.

Click [Uninstall Password] and a dialog box which shows "Uninstall Daemon Client Password" will display, select [Set Uninstall Password] to enter the password and click [Save] to save the configuration.

◆ **Uninstall**

Run the installation package of the client again and select uninstall. Enter the password in "please enter the uninstallation password" and click [OK] to finish uninstallation, or click [Cancel] to cancel the operation.

3.3 Linux Client

Linux client is deployed on Linux system to respond to the command of management console. It provides data backup for file, Oracle, and more to protect data on Linux platform. Only the daemon client is supported currently.

3.3.1 System Requirements

Item	Requirements (required)	Requirements (recommended)
CPU	1 GHz	2 GB or above
Memory	1GB	2 GB or above
Disk Space	28 MB	50 MB or above
OS	RedHat Linux Enterprise 4	RedHat Enterprise Linux 5(32/64bit) or later
NIC	100 Mb/s	1 Gb/s
Browser	None	IE 9.0 or Firefox 20

Figure 19 System requirements of Linux client

3.3.2 Installation Wizard

The installation package for the Linux client can be found in two ways: 1) Access to EISOO AnyBackup Appliance page through a web browser and download the Linux client. 2) Decompress the installation package and find the corresponding installation package for the Linux client in EISOO AnyBackup Appliance \Setup, then install as follows:

Step 1: Copy client.tar.gz to Linux environment and save in certain directory. In this example, in the /opt directory.

Step 2: Navigate to the /opt directory by using "cd opt/" command.

Step 3: Decompress the installation package by using "tar –xzf: AnyBackup _client_rht4.tar.gz", after decompression, a folder called [AnyBackupClient] will appear in the "eisoo" directory.

Step 4: Enter the AnyBackupClient directory by using "cd AnyBackupClient/" command and run the installation program by using "./install.sh" command.

Step 5: Select the language. Enter corresponding number and press [Enter] to continue.

Step 6: Enter the console IP and press Enter to continue.

Step 7: Select user type: only user, Oracle, Sybase, MySQL are provided. Enter the corresponding number and press Enter to continue.

Step 8: You will be asked whether to install trans.ko, which is used for disaster recovery. If yes, install and continue.

Step 9: All settings selected in the previous steps will be shown. Ensure it is correct before continuing installation. Enter y to start installation.

Step 10: After installation, check whether client is installed correctly by using "ps –e|grep eng" command, and all the above operations will be shown as follows:

Figure 20 Install Linux client

3.3.3 Uninstallation

Step 1: Log in to the Linux server and stop the running client.

Step 2: Navigate to the AnyBackupClient directory and use the "./uninstall" command to finish uninstallation automatically.

3.4 System Recovery Environment (SRE)

System Recovery Environment is the environment which can boot and execute the system recovery program independently when your system fails. It can run when computer starts without Windows, thus helping you to restore system when the system is down.

The SRE can run on CD and USB device independently, thus simplifying system restore. For ease of use, a graphical interface is available. It supports direct LAN access, thus enabling centralized backup and restore.

3.4.1 System Requirements

Item	Requirements (required)	Requirements (recommended)
CPU	900 MHz	1.2 GHz or above

Memory	512 MB	1 GB or above
Disk Space	200 MB	400 MB or above

Figure 21 System Requirements of SRE

3.4.2 Installation

If you do not have the CD, you can configure SRE by using the installation program.

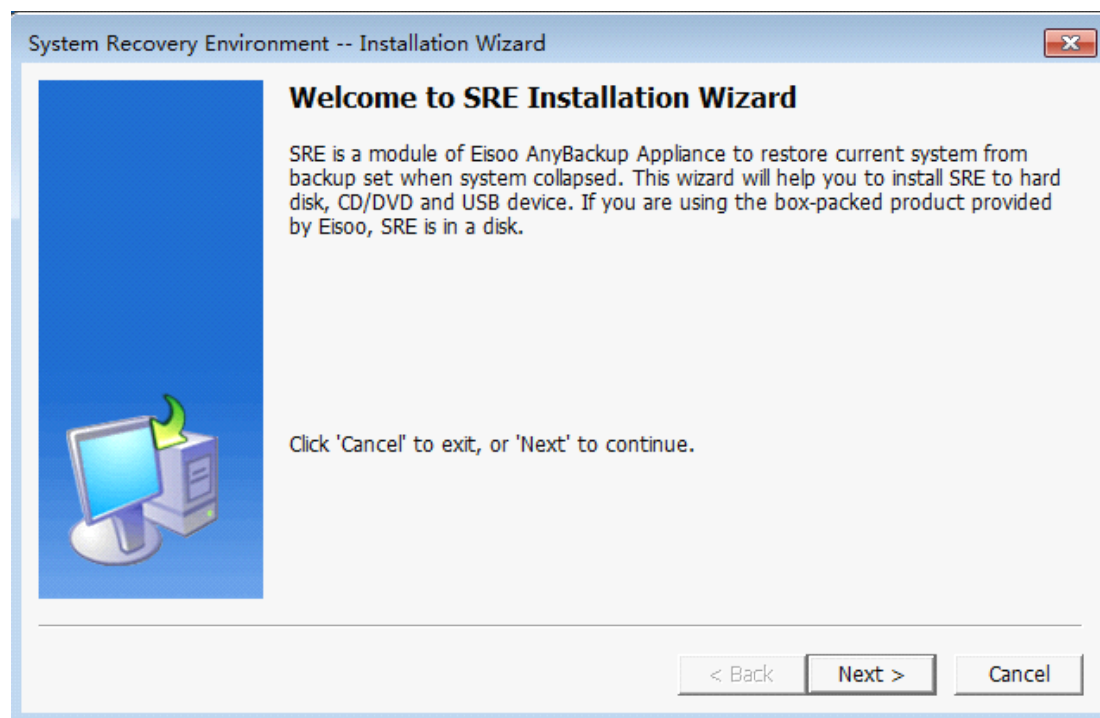Step 1: Select the installation file according to system. Enter installation wizard and click Next;

Figure 22 Install SRE step 1

Step 2: Select to install by using USB device or CD, here the USB device must have an active FAT/FAT32 partition. Then click [Next];
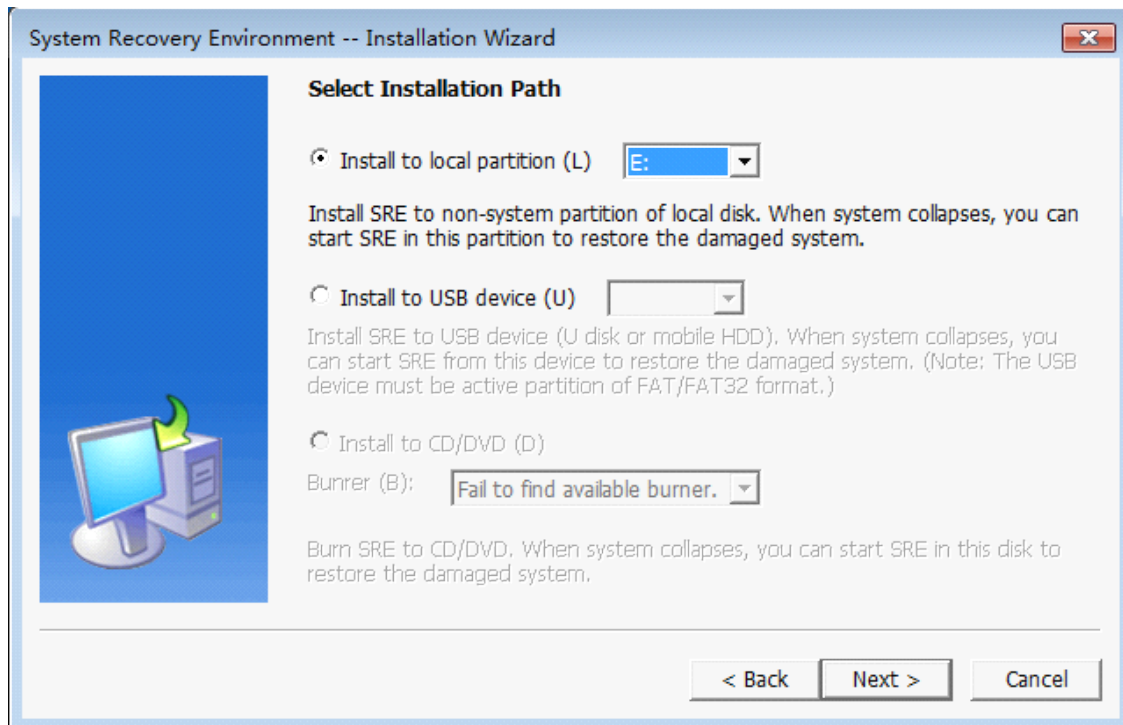
Figure 23 Install SRE step 2
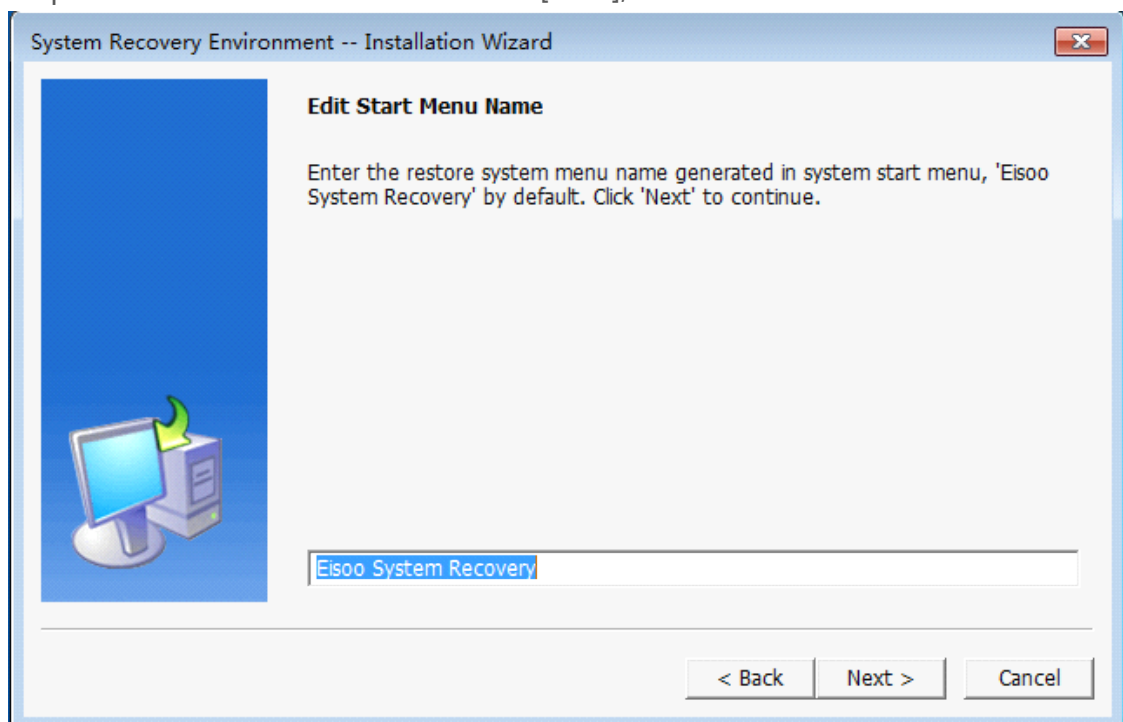
Step 3: Edit Start Menu Name and click [Next];

Figure 24 Install SRE step 3

Step 4: Start to copy the files for SRE, click [Finish] when it finishes and the installation ends.
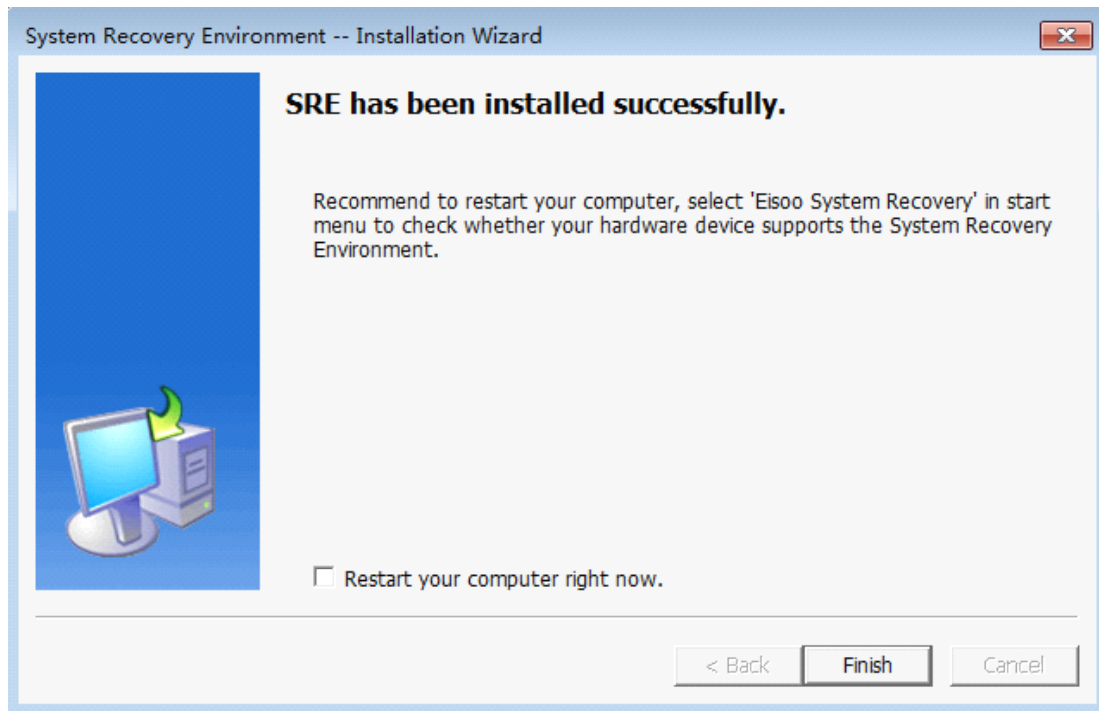
Figure 25 Install SRE step 4

3.4.3 Boot SRE

◆ **Via USB**

If you have installed SRE in a USB device, you can boot from this device.

Step 1: Start computer and set in CMOS\bios to ensure the default boot media is USB drive.

Step 2: Connect the USB device to the computer.

Step 3: USB drive is detected and start to boot, "Boot" will display.

Step 4: Press Enter and SRE boots.

◆ **Via CD Disk**

If you have the CD/DVD, you can boot from it.

Step 1: Start the computer and configure in CMOS\bios to ensure the default boot media is CD-ROM.

Step 2: Insert the disk to CD-ROM.

Step 3: Disk is detected and start to boot, "Boot" will display.

Step 4: Press Enter and SRE boots.

Chapter 4 Centralized Management

This chapter will introduce how to manage the AnyBackup Appliance over the network. including centralized management, backup and restore management based on console, disaster recovery and system management, storage and device management based on media server. Here we introduce the home interface and how to centrally manage the device via root nodes.

4.1 About Home

4.1.1 Home of Management Console

The homepage of management console, whose primary purpose is to display the product info, enterprise info, client security status and client info, is shown below. Log in to the management console and click "Management Console" on the left, and you will see the following interface:
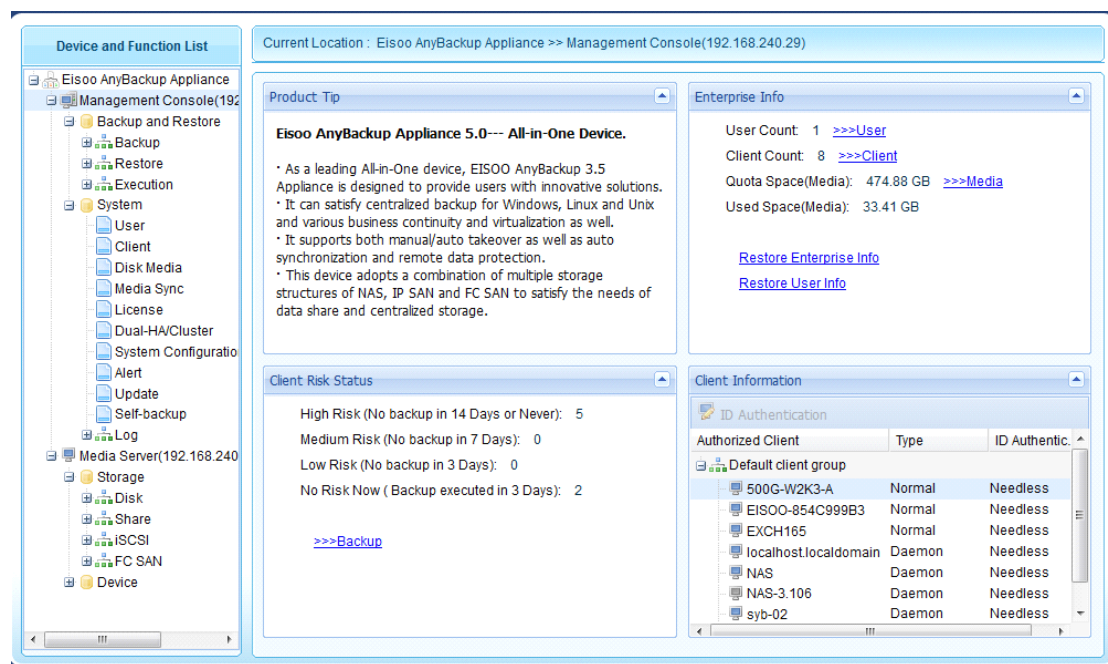

Figure 26 Home of Management Console

4.1.2 Home of Media Server

Here we introduce the homepage of media server, which displays the status of this server, including system status, hard disk status, RAID status and Storage space. Log in to the management console and click "Media Server" on the left, and you will see the following interface:
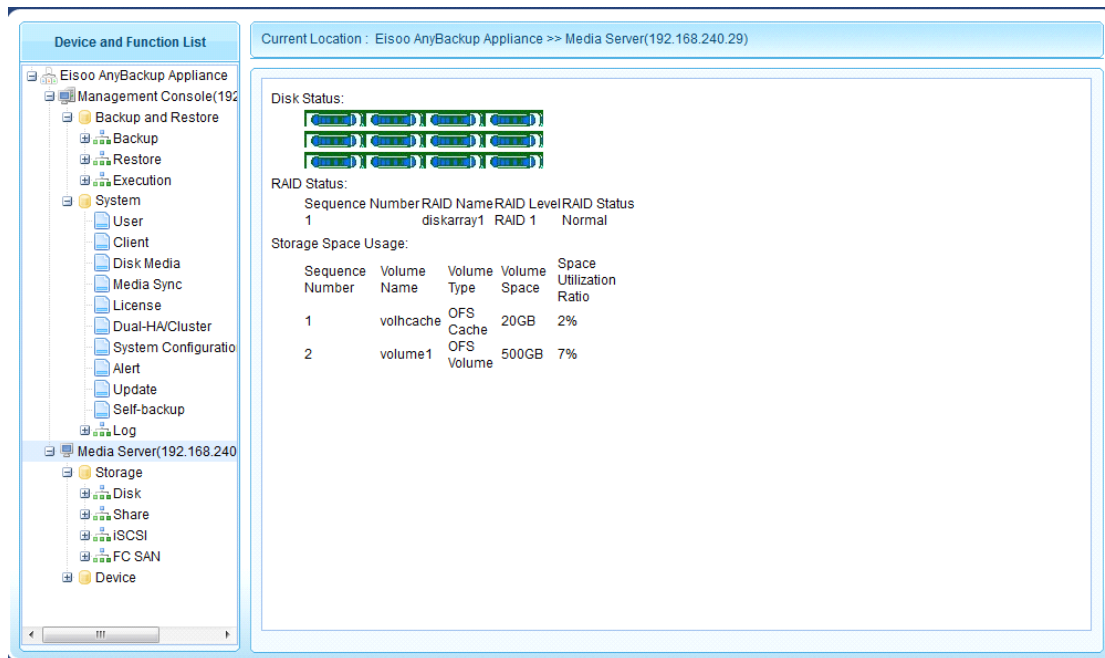
Figure 27 Home of media server

4.2 Centralized Management

For centralized management of backup devices, AnyBackup Appliance provides one interface to manage multiple devices. Log in to the AnyBackup Appliance and you will see its interface. Click root node "AnyBackup Appliance" and you will see the device model, IP and system status if logging in by admin account:

Figure 28 Centralized Management

◆ **Refresh**

Click [Refresh] and the status of device in the list will update automatically.

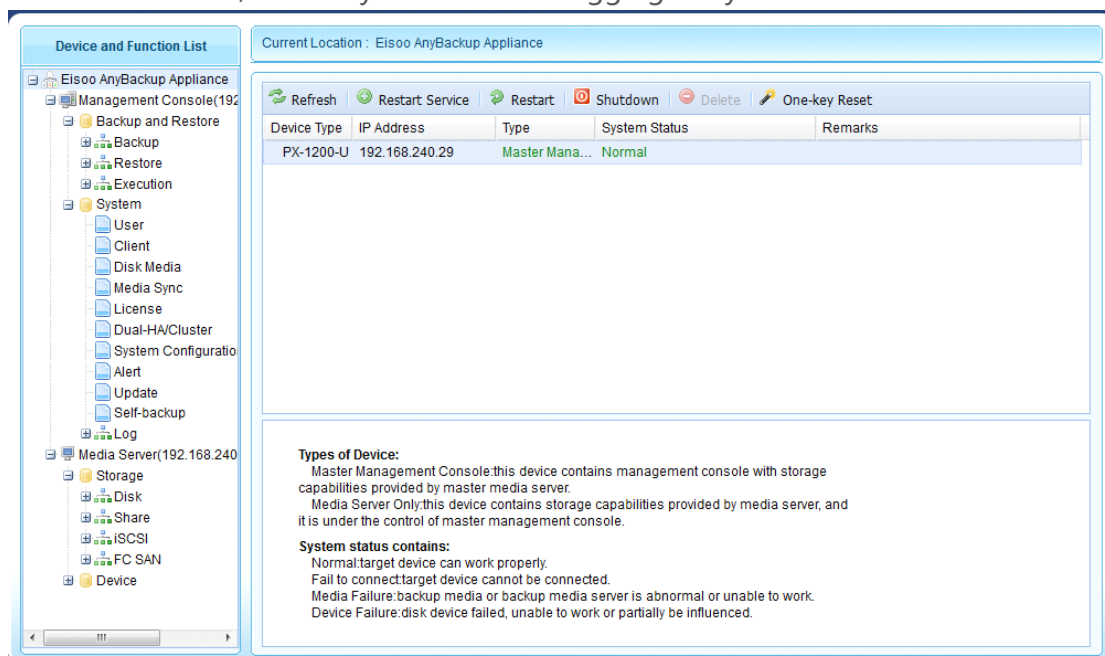◆ **Restart Service**

Select the device for service restart and click [Restart Service].

➢ Click [Yes] in the confirmation window to restart service of the device.

➢ Click [No] to return to the main interface.

◆ **Restart Device**

Select the device to be restarted and click [Restart Device].

➢ Click [Yes] to restart the device.

➢ Click [No] to return to the main interface.

◆ **Shutdown Device**

Select the device to be shut down and click [Shutdown Device].

➢ Click [Yes] to shutdown the device.

➢ Click [No] to return to the main interface.

◆ **One-key Reset**

One-key reset is used to resume software to default configuration, not including network configuration, media server configuration (storage management, device management), authorization configuration, self-backup info saved in default path, and more. Before one-key reset, we recommend you to perform self-backup. When it finishes, it will skip to configuration wizard automatically.

Chapter 5 System Management

5.1 User Management

Users are the foundation for using AnyBackup Appliance. A username should be set to log in to the management console to perform data backup and restore for authorized client and media server. Users are created by the administrator in "System/User" where the admin can create/modify/delete user (group), import domain users, give authorization to clients, etc.

In AnyBackup Appliance, user info includes:

➢ Username: used to log in to the console and execute data backup and restore for authorized clients and media server.
➢ Description: notes configured while creating user.
➢ User Type: type of user, such as audit admin, user, etc.
➢ User Group: group the user belongs to.
➢ Status: status of user; enabled or disabled.
➢ Authentication: to decide whether the user logs in to the console based on password, USB-Key or password & USB-Key.
➢ Free Space: Available space for the user.
➢ Used Space: Storage space used by this user.

5.1.1 Create and Manage User

◆ **Create User**

Click [New] and enter a username, description, user group, authentication type and space limit in the dialog as shown:

Figure 29 Create user

Click the [Authentication Type] drop-down menu and you will see the following three types:

- ➢ Based on Password: Default password is 123456 and can be modified after logging in as this new user.
- ➢ Based on USB-Key: Insert the USB-Key got from EISOO to bind with this user.
- ➢ Based on Password and USB-Key: Insert the USB-Key got from EISOO to bind with this user. After binding successfully, the USB-Key must be inserted when logging in, and then the user password, which is 123456 by default, must also be entered.

◆ **Modify User**

Select a user and click [Modify] to edit description, user group, authentication type and space limit. Click [OK] to finish modification.

◆ **Delete User**

Select a user and click [Delete]. Click [Yes] to delete user or [No] to cancel.

If job of the user is executing, the request will fail, please manually stop the job first or wait until it finishes.

◆ **Import Domain User**

Before importing a domain user, make sure the LDAP assistant has been installed. Click [Import User] and select a user in the Windows domain user list and click [Yes] to finish importing.

◆ **Register User**

When an admin marks "Register User", ordinary users are allowed to register on the login page. The newly-registered user will be added to the user list of admin and will be given related authorizations.

5.1.2 Create and Manage User Group

◆ **Create User Group**

Create new group for unified management of users belonging to one department. Click [User Group]>>[New] and enter group name, description and select user to the new group by clicking >> or <<. Then click [OK] to finish.
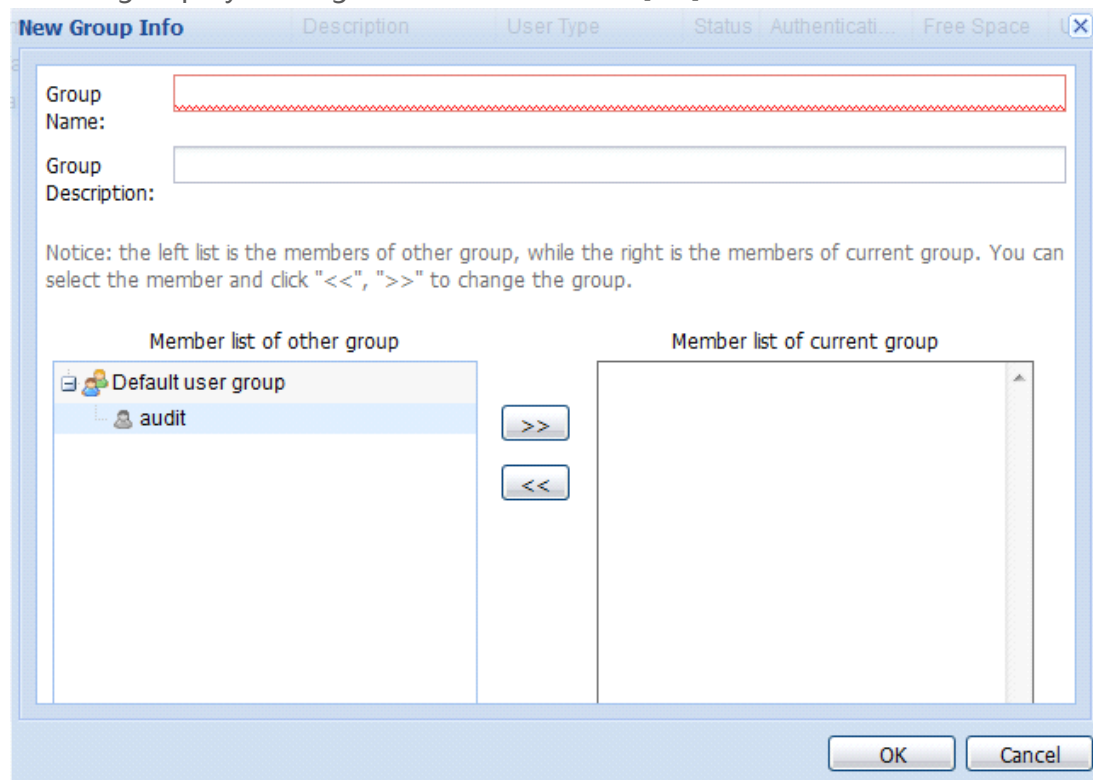

Figure 30 Create user group

◆ **Modify User Group**

Modify group name, description and attributes of group members.
Select the group to be modified, click [User Group]>>[Modify]. You can enter the new group name and description, or click >> or << to change the attributes of users. Finally, click [OK] to finish modification.

◆ **Delete User Group**

Select the group to be deleted and click [Delete]. Read the instructions carefully and click [OK] to finish deletion.

5.1.3 Configure User Authorization

Authorize the current user to back up data of specified client and to read/write to data of specified media.

◆ **Client Authorization**

Select one user (group) and click [Authorization], and the window of default client authorization will display. Select any client or client group in the unauthorized list and click the button of "<<" to change it to the authorized list. Then click [OK] to finish authorization.
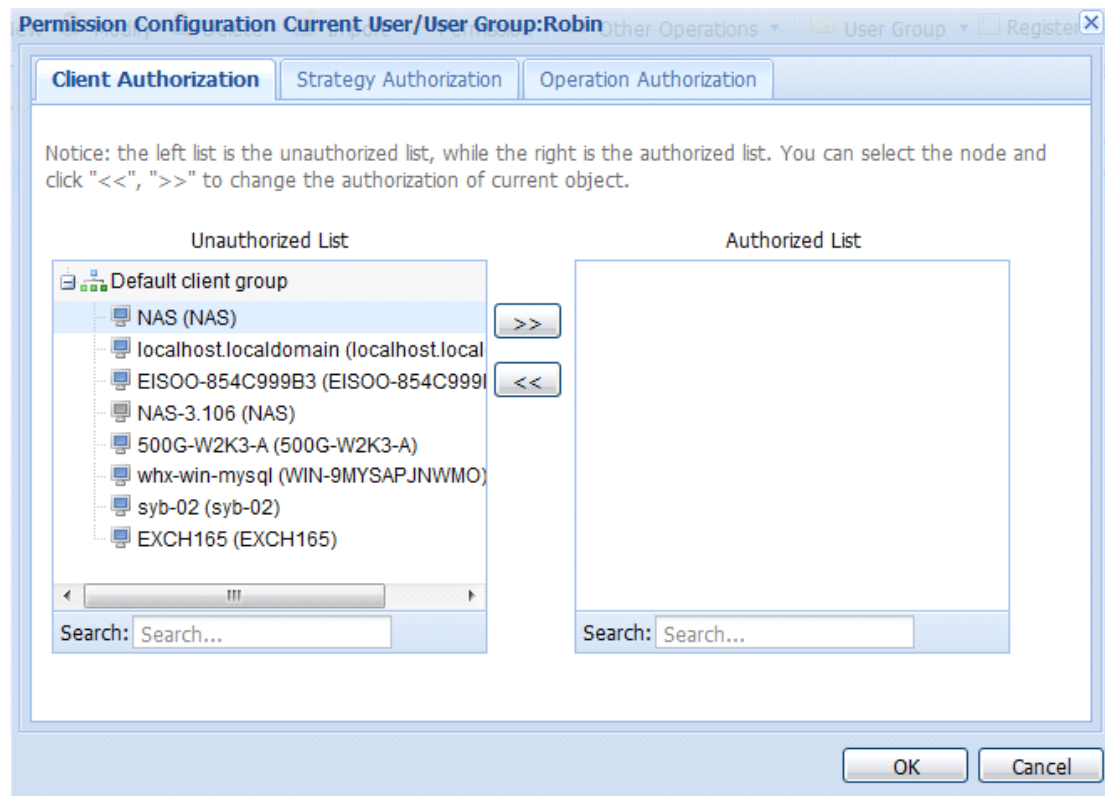

Figure 31 Client authorization

◆ **Strategy Authorization**

Switch to strategy authorization, select any strategy in the unauthorized list and click ">>" to move it to the authorized. Click [OK] to finish authorization.
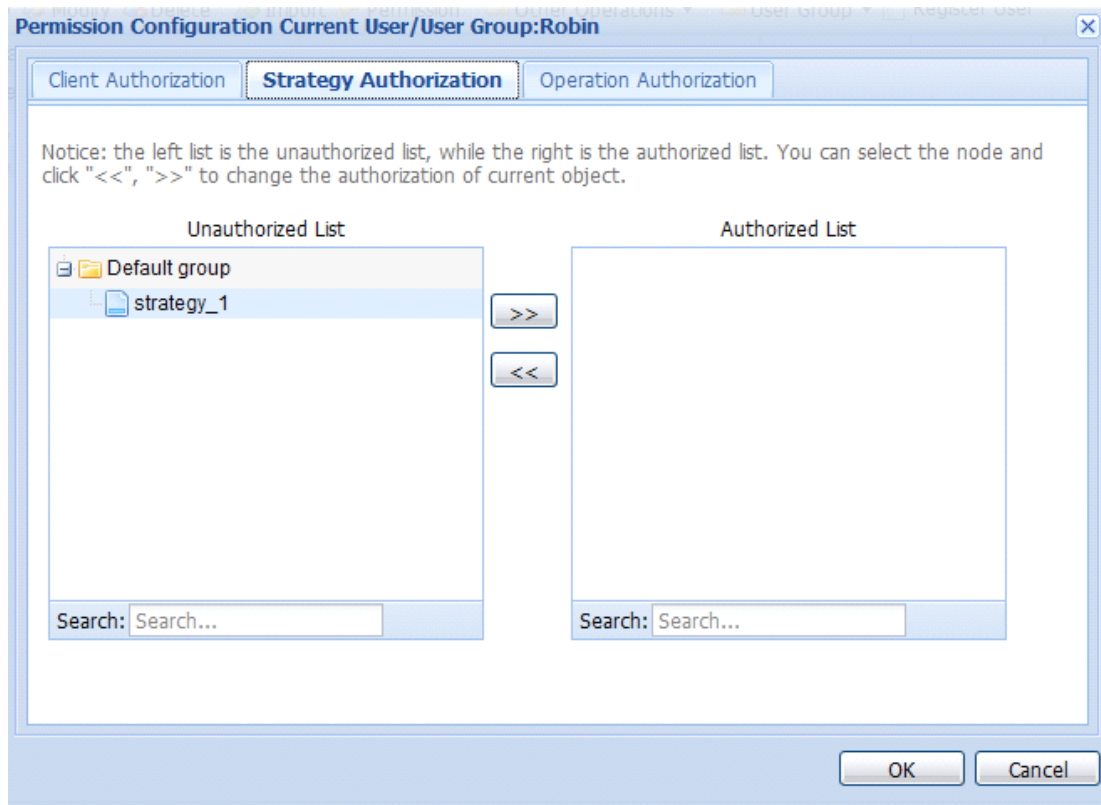
Figure 32 Stategy authorization

◆ **Permission Authorization**

Click permission authorization and select the type to be changed in the authorized list and click "<<" to move it to the unauthorized list. Click [OK] to finish configuration.
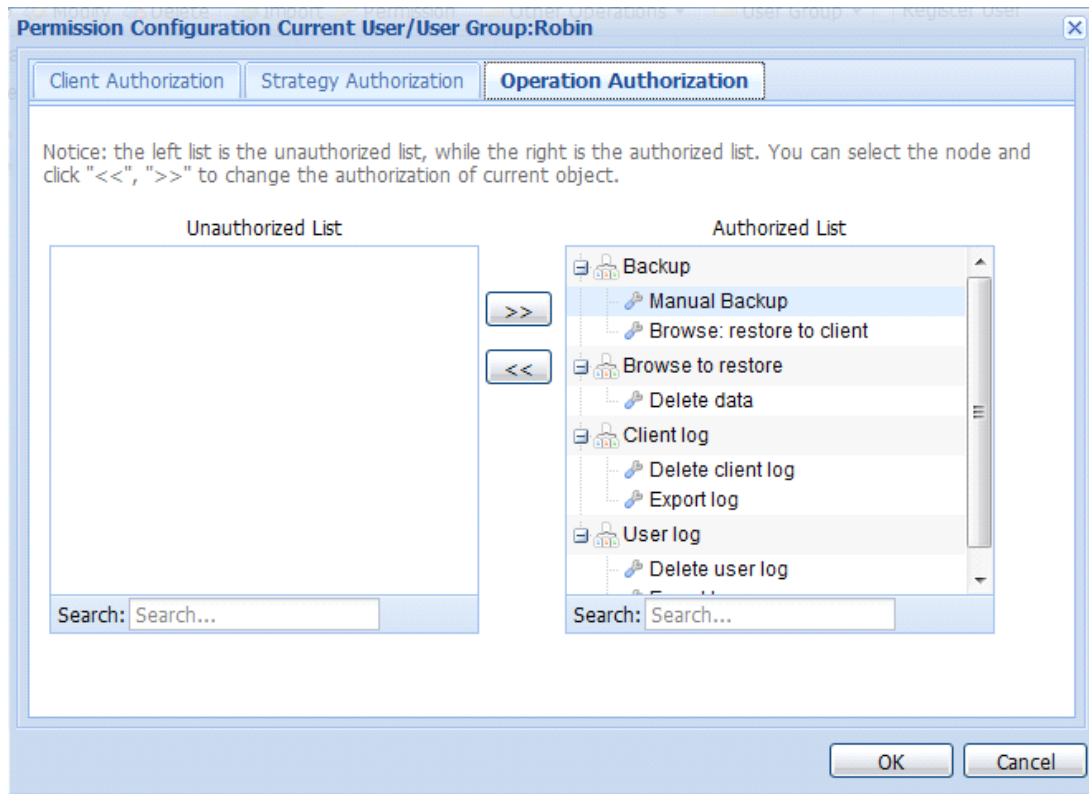
Figure 33 Operation authorization

5.1.4 Other Operations

Click other operations and you can enable/disable user (group), reset password, etc.

◆ **Enable**

If the user (group) is disabled, select this user (group) and click [Enable] to resume its status.

◆ **Disable**

If you want to disable the user (group), select the user (group) and click [Disable] and its label will turn grey. The user (group) cannot log in to the console while disabled.

◆ **Reset Password**

Useful in two situations, one is when a user forgets the password and the other is when the user resigns.

Select the user and click "Reset Password". The original password cannot be used if it is reset. After resetting, an email will be sent to the administrator which contains user name, new password, and reset time. At the same time, this operation will be written to the audit and system logs, including user info, but not the password.

Password resetting is not supported for domain user, batch password resetting is not supported for user groups.

5.2 Client Management

Admin can group current clients, modify client groups, delete unnecessary client (group)s, bind user for secure client, specify database for current client, etc in "Client".

5.2.1 Client Group Management

Log in to the Management Console and click "System/Client".

◆ **Refresh**

Show the client group information.

◆ **New**

Create new client group.

◆ **Modify**

Modify group name, description, etc.

◆ **Delete**

Select a client group to be deleted and click [Client Group]. Select [Delete] in the drop-down list and click [Yes] in the confirmation window to delete the client group.

5.2.2 Configure Client

Click [Configure] and the following dialog box will display:

◆ **Priority**

Client priority refers to execution sequence of clients, including lowest, low, normal, high and highest.

◆ **Database Type**

Multiple databases are provided; you can mark the options to specify the database type for the client to back up.

◆ **Detection Time of Network Broken**

Configure the detection time of network broken, including 1, 3, 5, 10, 15 min, or you can manually enter any integer between 1 and 30.

5.2.3 Delete Client

Select the client to be deleted and click [Delete]. Read the instructions carefully and click [Yes]. The related configurations will be deleted as well.

After deletion, the client will not be in the authorized list or unauthorized list. When you want to reconnect it to the Management Console, you need to reconfigure server IP and client authorization.

5.2.4 Configure Virtualization

Select the client to be virtualized and click [Virtualization].
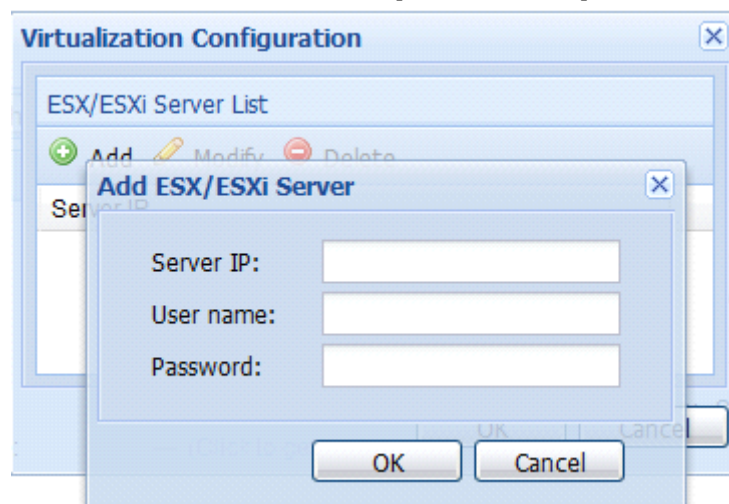

Figure 35 Configure virtualization

You need to add the IP, username and password of virtual platform manually, and make sure it is corrected or it will fail when creating a job.

5.3 Disk Media Management

Disk media management provides management and operation for multiple media servers of AnyBackup Appliance. Besides installation of master media server and

sub media server, administrators can also add extra media to store backup data, modify/delete media (server) and configure quota of specified storage space in [System]/[Media Server].

5.3.1 Operations of Media

◆ **Add Media**

Add new media on the selected media server.

- ➢ Server Name: Select the default media server or sub media server name.
- ➢ Media Name: The media name to be added.
- ➢ Storage Path: Path to save backup data on media server.
- ➢ Media Space: The maximum backup space of this media on media server. If backup data reaches the limit, new data cannot be written into the storage path of the media.

Select the server and click [Add]. Enter the media name, storage path, media space and click [OK] to finish media adding.
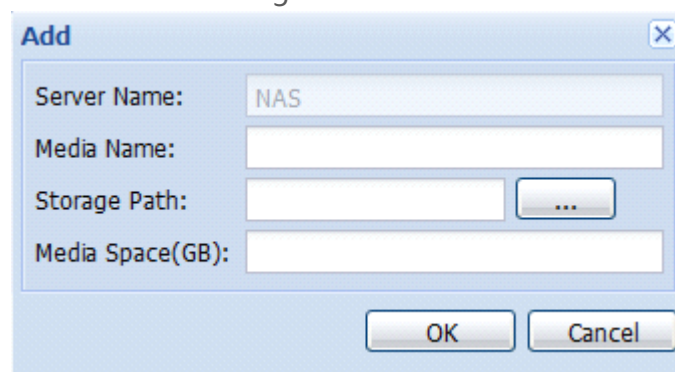

Figure 36 Add media

◆ **Modify Media**

Select the media server and click [Modify] to modify the size of media space. Click [OK] to finish modification.

◆ **Delete Media**

Select the media and click [Delete]. Click [OK] to finish deletion.

5.3.2 Operations of Media Server

◆ **Modify Media Server**

Select one media server to modify its configuration info.

- ➢ Server Name: The media server name configured when installing media server. It can be modified.
- ➢ Storage Port: the port used for media server to change working status with other modules, such as client. It is 9902 by default and can be changed if necessary.
- ➢ IP address: the IP address for client to access to the media server.

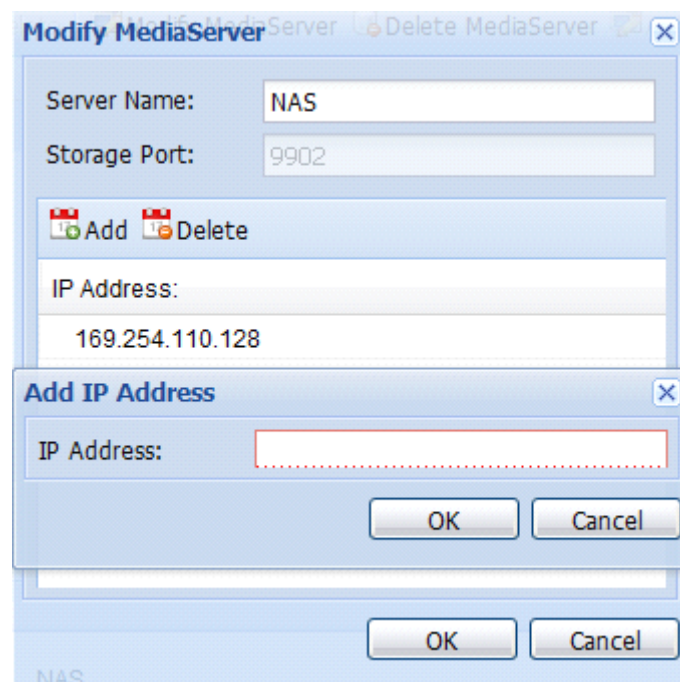Click [Modify] and [Yes] to modify name and IP of the media server. Then click [OK] to finish modification.

Figure 37 Modify media server

◆ **Delete Media Server**

Select certain media server and click [Delete]. Choose [Yes] to finish deletion.

5.3.3 Backup Configuration of NAS Media

Step 1: Map the network path of media (NAS or others) to the media server.

➢ Open [My Computer] and click [Map Network Drive] on the toolbar.

➢ Enter the file name to be mapped and the storage path. Then click [OK].

➢ After it finishes, [Network Drive] will be displayed in [My Computer].

Step 2: The currently running account of media server is the local system user. If you want to add the network mapping disk as the media storage path, log in to media service via the current user ID.

➢ Click [Start] and open the [Control Panel]. Select [Service] in [Management Tool].

➢ Select AnyBackup MediaServer in [Service] and configure [Login] as [This Account]. Then click [OK] to finish.

Step 3: Add media in [Media] and configure shared disk path as media path.

➢ Click [Add] in [Media].

➢ Enter media name, add storage and select the network mapping disk in [Add]. Click [Yes] to finish.

5.3.4 D2D2R Authorization

Authorize media sync server to use remote console. When host or authorized

console fails, you can restore enterprise information and user information by using the media server or media sync server.

Step 1: Log in to the host console and select the media sync server to be authorized. Click [Authorize Console] and add the console IP to be authorized. If you want to remove the authorization, select the IP address and click [Delete].
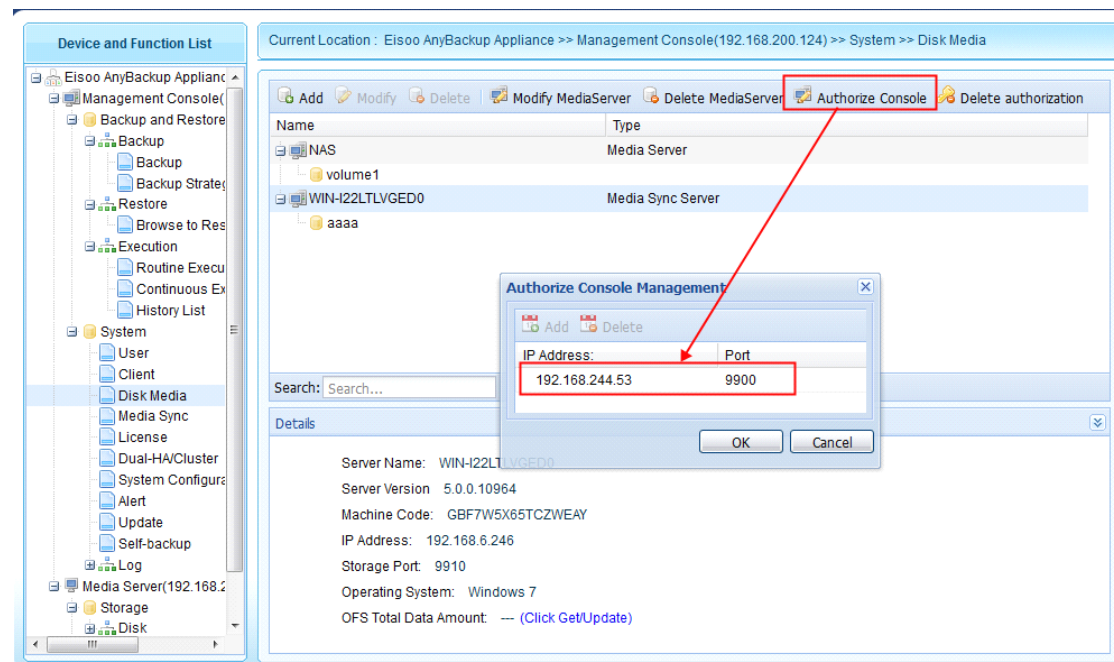

Figure 38 Add IP address of the console to be authorized

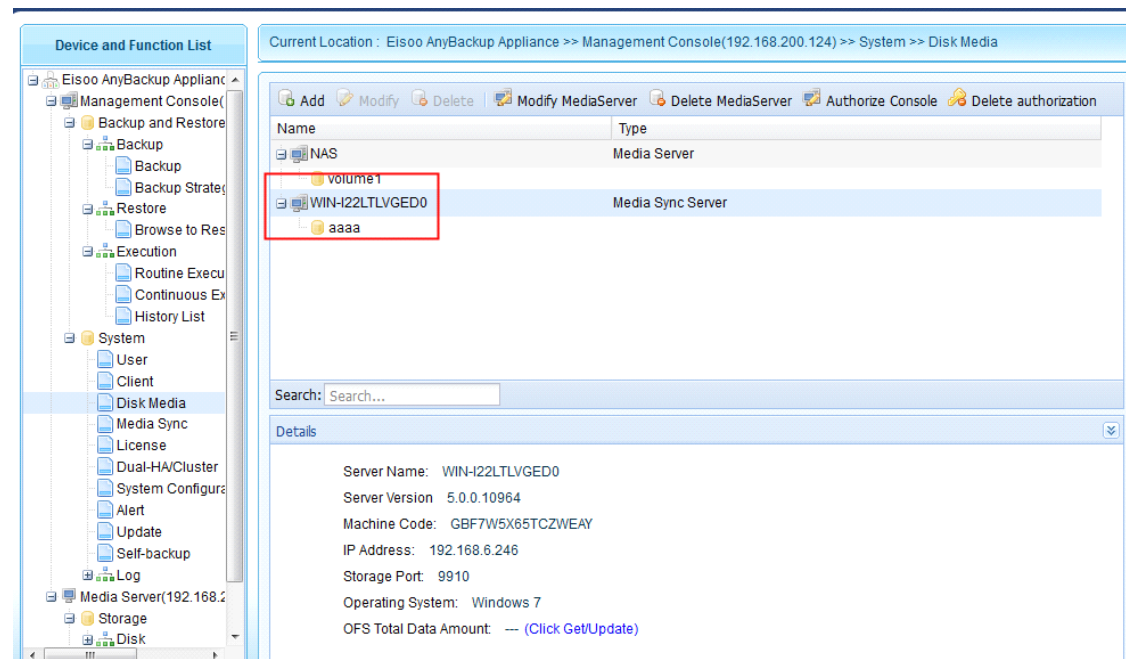Step 2: Log in to the authorized console and the authorized media sync server is connected.

Figure 39 Connect media sync server

Step 3: Create console and finish installation wizard.

Step 4: Users can restore console via media sync server or media server, just as the following figure shows. First, stop the media service and modify mediasvrsetting.config under AnyBackup/console, and then change the console IP to new console IP. Restart the media service.

Step 5: Log in to the new console and the connected media server and media sync server are listed in "Disk Media".

Step 6: Select xxx user of xxx console to be restored in "Restore User Info" and pass the password authentication and restore will complete. Select IP of xxx console in "Restore Enterprise Info" and pass the password authentication, and all backup data on this console will be restored. The backup data set can be browsed in "Browse to restore".

Step 7: Select the IP address of host console (authorized console) to be restored. If restoring via media server, select IP address to be restored in "Media Server".

Step 8: Enter the password to log in to the host console (or authorized console) to finish restore.

5.4 Media Sync Management

5.4.1 Overview

Media Synchronization is mainly used to synchronize backup data among media, which means to synchronize local latest data to specified remote media sync server to realize remote disaster recovery. AnyBackup Appliance supports synchronizing backup data on one media to one or multiple media, but not among media on the same media server.

ᗧ Note: Before creating a media sync job, ensure the remote media server has been deployed.

5.4.2 Operations

◆ **Create Media Sync Job**

Step 1: Click [New Sync Job] and enter job name. Respectively select the media server for data synchronization in "Source Media Server" and "Target Media Sync Server".
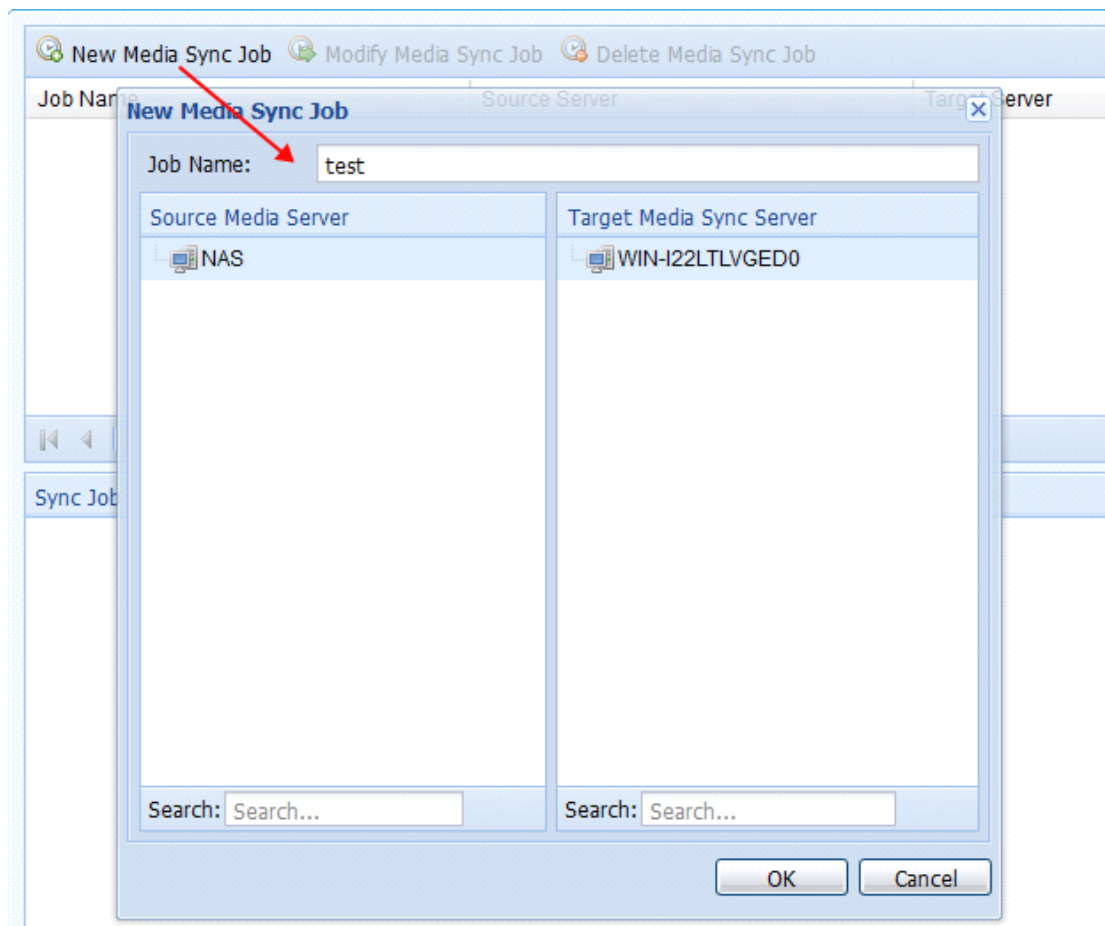
Figure 40 Create media sync job

Step 2: Click [OK] to finish media sync job creation.

◆ **Modify Media Sync Job**

Step 1: Select the sync job to be modified and click [Modify].

Step 2: Modify job name, source media server and target media server.

Step 3: Click [OK] to finish modification.

◆ **Delete Media Sync Job**

Select the sync job to be deleted and click [Delete]. Choose [Yes] to stop the sync job.

◆ **Reverse Direction Media Sync**

Reverse direction synchronization is a supplement for media sync. When local data is lost, you can restore to local data center by using the data on a remote media sync server.

Step 1: Select the media sync server for reverse direction sync. Then click "Restore to Media Server" under [Operation].
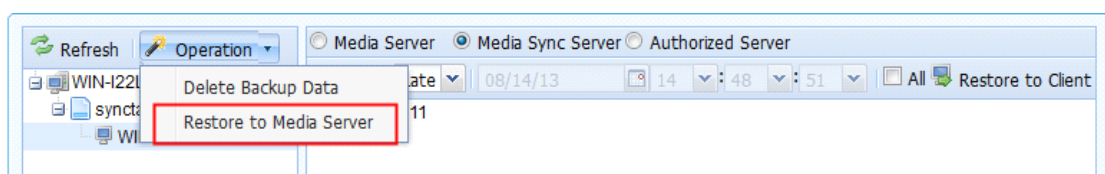
Step 2: Select the media server to be restored to and click [OK]. Click [OK] in the warning window.

The job will be displayed in [Routine Execution] if submitted, with job type as "Reverse Direction Media Sync".

◆ **Breakpoint Resumption**

When target media server stops by exceptions such as insufficient space, offline, power interruption, network broken during media sync job, "Running (execution error, please check details)" will be displayed in the media status. When the problem is fixed, the job will continue execution with no need to restart.

5.5 License Management

In AnyBackup Appliance, each client needs to be authorized. Log in to the console and click "System/License" to add, delete license, authorize to manage clients and activate license, etc.

5.5.1 Add and Delete License

◆ **Add License**

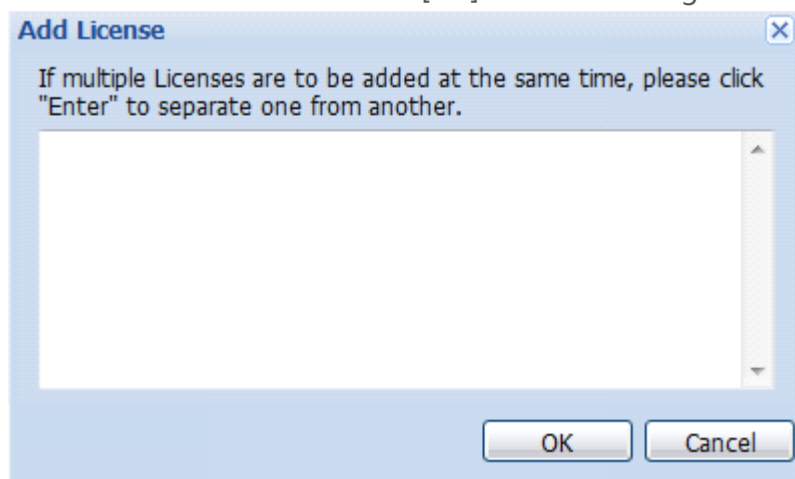Click [Add] to enter the license. Then click [OK] to finish adding.

Figure 42 Add license

◆ **Delete License**

Select a license and click [Delete]. Read the confirmation alert carefully and click [OK] to finish deletion.

Ď **Note:** You need to add the license of a basic module first, then add licenses of other modules and activate them. If you want to delete the license of a basic module, delete other modules first.

5.5.2 Activate License

When registered successfully, the product will auto log in to Eisoo server to record the license you entered. You need to activate your license in 30 days after registration; otherwise the product will not be usable.

◆ **Online Activation**

Select the license to be activated and click [Online activation]. Its status will change to "Activated".
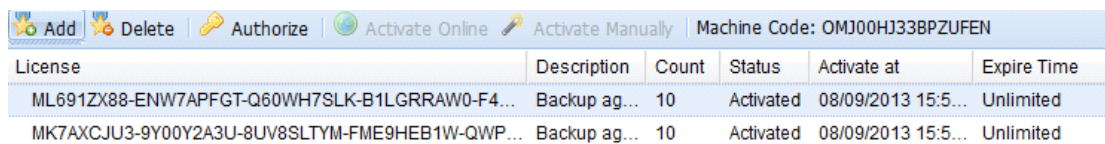
◆ **Manual Activation**

If online activation fails due to network problems, please use manual activation.

Select the license to be activated and click [Manual Activation]. Enter the license and click [OK] to finish.

5.5.3 License Authorization Management

License authorization management is used to authorize remote agents after license is added, for example, to authorize desktop email backup for remote clients.

Step 1: Enter [License] and select the desktop email backup agent license to be authorized.

License	Description	Count	Status	Activate at	Expire Time
ML691ZX88-ENW7APFGT-Q60WH7SLK-B1LGRRAW0-F4...	Backup ag...	10	Activated	08/09/2013 15:5...	Unlimited
MK7AXCJU3-9Y00Y2A3U-8UV8SLTYM-FME9HEB1W-QWP...	Backup ag...	10	Activated	08/09/2013 15:5...	Unlimited

Machine Code: OMJ00HJ33BPZUFEN

Figure 43 License authorization

Step 2: Click [Authorization Management] and the "Authorize remote agent" window will display.

Step 3: Click ">>" or "<<" to change the authorization status of the selected client.

Step 4: Click [OK] to finish.

> **Note:** License authorization management is for licenses of agents only, but not for license of basic module and options.

5.6 Dual-HA/Cluster Management

Log in to the console by using an admin account and you can create/modify Dual-HA/Cluster binding in [Configuration]\[Dual-HA/Cluster].

◆ **Create Dual-HA Binding**

Click [New Dual-HA Binding] and you can configure binding name, description, and floating IP. Floating IP means the IP for external services on dual-HA. It allows the

program to decide whether the device is a host. Move a client from the unbound list to the bound list and click [OK] to finish binding.
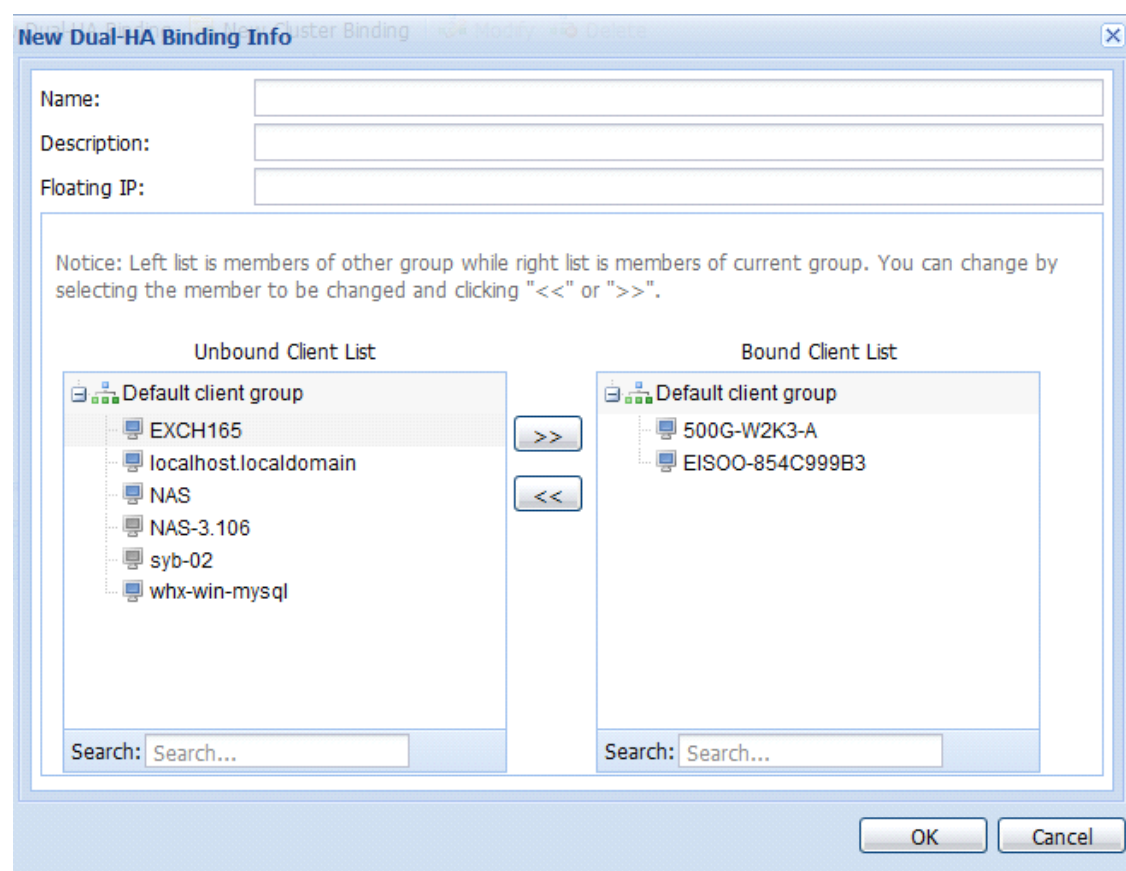

Figure 44 Create Dual-HA binding information

◆ **Create Cluster Binding**

Click [New Cluster Binding] and you can configure binding name, description, and select whether to set the archive path on each node. Move the client from the unbound list to the bound list and click [OK] to finish binding.
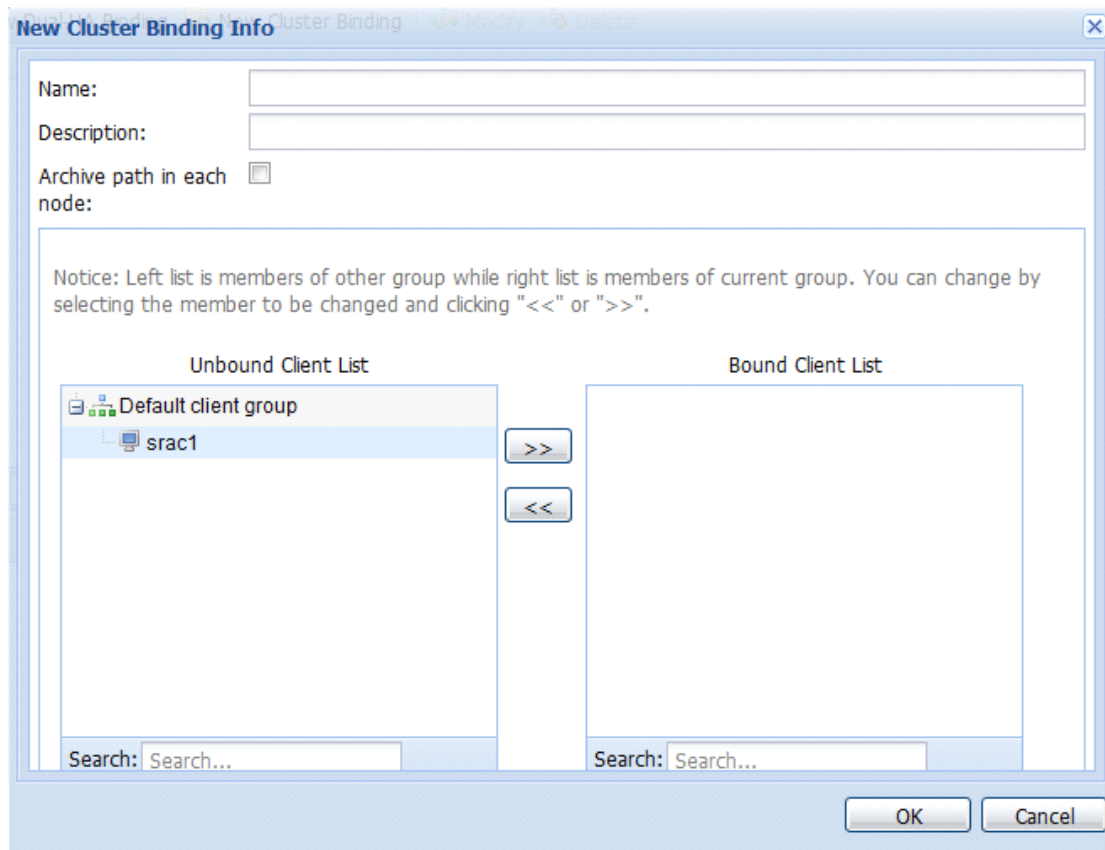
Figure 44 Create Cluster binding information

◆ **Modify Binding**

Select the bound Dual-HA/Cluster group and click [Modify] to modify binding name, description and the bound client.

◆ **Delete Binding**

Select the Dual-HA/Cluster group and click [Delete]. Click [Yes] to finish deletion, or [No] to cancel. If binding is deleted, all related configurations and backup jobs will be deleted.

5.7 System Configuration

Click "Management Console/System Management/System Configuration" and you will see the following information:

◆ **Service Info**

Click [Modify] on the right and you can modify the network address and port of the server, usually used for multi-NIC environments or port conflict.

◆ **Email Configuration**

Used to configure server end to send email notifications to bound mailbox. Click [Modify] in the right to configure SMTP server address, port, email and password.

◆ **Execution Queue**

Click [Modify] in the right to configure the maximum job count which can be executed simultaneously.

◆ **Auto Cleanup**

You can retain the logs and execution histories in the time period configured. Click [Modify] in the right and enable auto cleanup. You can select to retain user, client and system logs and execution history list for 2 years, 1 year or half a year.

◆ **Uninstall Password**

Click [Modify] in the right to configure the uninstallation password of Daemon Client.

◆ **Forbid to Execute**

Click [Modify] in the right to configure/modify/delete the time period when execution is not allowed. During this period, all execution items of all users will be stopped, together with all execution items scheduled.

◆ **Temporary Data Path**

Click [Modify] on the right to configure the temporary storage path for default media server and restore server of this console.

◆ **Auto Creation Rule of Shared Directory**

Click [Modify] on the right to configure auto creation of shared directory when creating/importing users.

◆ **Site Configuration**

Used to configure configuration info and site type to connect to Tx3 Cloud Platform.

◆ **Site Public Network IP**

One public network IP can be configured when site is in intranet. The authorized media sync server can connect to site by using this IP.

5.8 Warning Configuration

Warning configuration provides email warning, sound warning and remote email warning to send the warning details to the system administrator. The warning details include hard disks being offline, hard disk failure, hard disk full, etc. Click "System/Warning" to enter the following page:
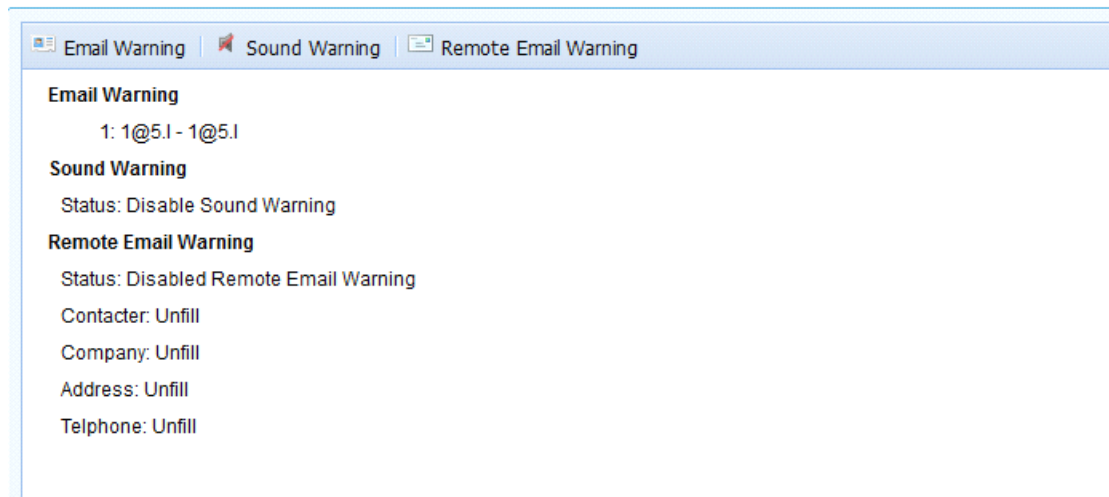
Figure 45 Warning configuration

◆ **Email Warning**

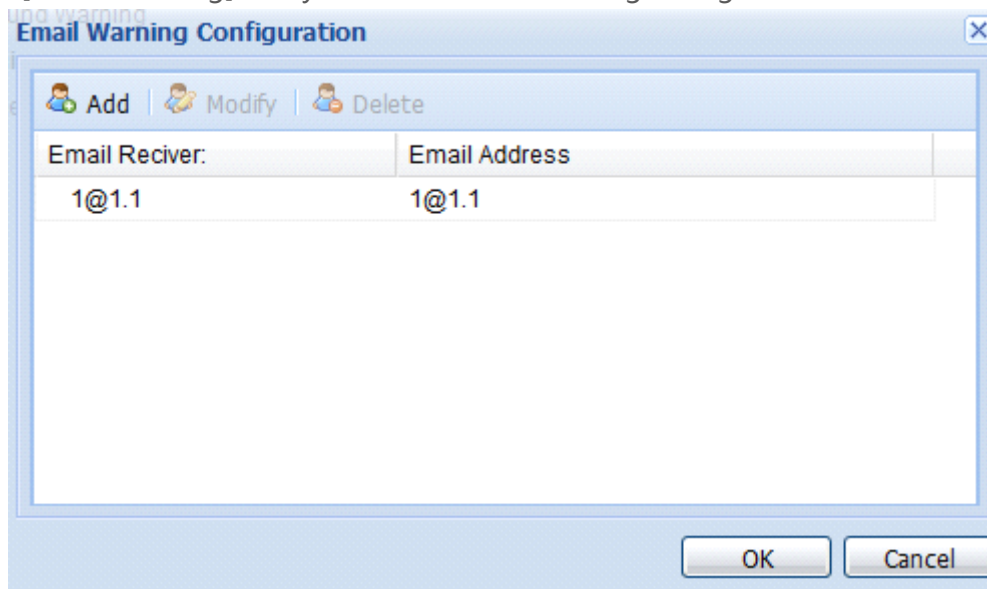Click [Email Warning] and you will see the following dialog box:

Figure 46 Email Warning

➢ Click [Add] to add email receiver and email address which are both needed. Email address can only be composed by A~Z, a~z, 0~9 and @ (e.g. yourname@domain.com).

➢ Select an email receiver and click [Edit] to modify email receiver and email address. Enter the new details and click [OK] to finish. Or you can click [Cancel] to return without saving.
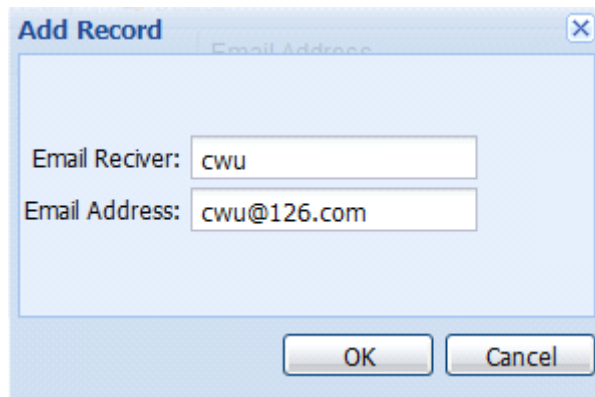
Figure 47 Edit record

➢ Select an email receiver and click [Delete]. Select [Yes] to finish deletion or [No] to return without saving.

➢ Click [OK] to finish configuration of email warnings, or [Cancel] to return without saving.

◆ **Sound Warning**

Click [Sound Warning] and you will see the following dialog box:
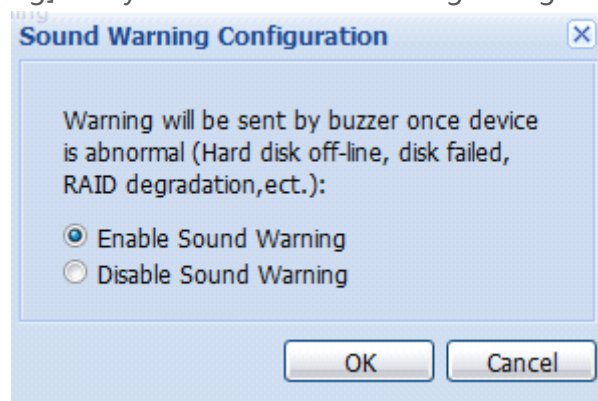
Figure 48 Sound Warning

➢ Sound warning is disabled by default, the button is grey.

➢ Select "Enable" and click [OK] to save configuration. Or click [Cancel] to return without saving.

◆ **Remote Email Warning**

Remote email warning is used to send the warning details by email to EISOO global monitor function, where the contact user is included. Once the warning details are received, EISOO will notify users immediately. Click [Remote Email Warning] and the following will be shown:

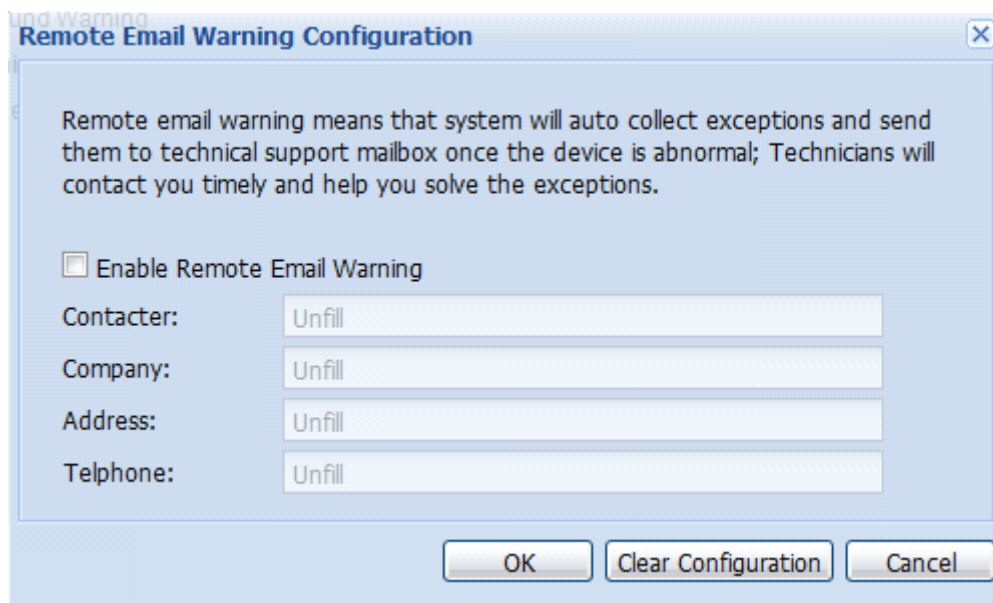**Figure 49 Remote Email Warning**

➢ Mark "Enable Remote Email Warning" and enter correct info here. Click [OK] to finish operation, or [Cancel] to back.

➢ Click [Clearup] and all information will be cleaned.

5.9 Update Management

Log in to the console by using the admin account and check update/import update package/delete update package/configure update in "System/Update" for unified update management.

◆ **Configure Update**

Click [Configure Update] to configure update package storage path, default as installation path and click [OK] to save.

◆ **Check Update**

Click [Check Update] and the packages will be shown. Click the link you want to download and save to the specified path.

◆ **Import Update**

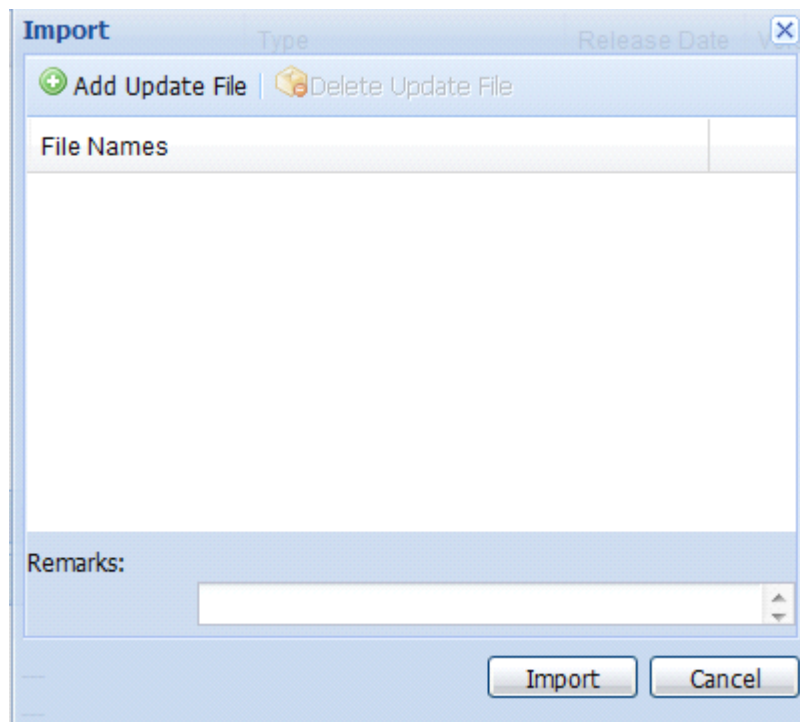Step 1: Click [Import Update] and the following will display:

Figure 50 Import Update Package

Step 2: Click [Add Update File] to select the package for update.Step 3: Click [OK] to finish import.For convenience, we recommend that you add comments to update packages.

◆ **Update**

➢Click [Update] and select specified client. Then click [OK].

➢Click [Yes] to deliver package and update. Click [Cancel] to cancel update.

■ Click any update package and it will show its type, release date, size, version, range, remarks and description.

■ After update, update report will display automatically to show result.

◆ **Delete Update Package**

Select the update package to be deleted and click [Delete]. Click [OK] to finish deletion or [Cancel] to return without saving.

5.10 Self Backup Management

AnyBackup Appliance supports backing up management console server settings, including database info (backup job, log info, media server info, etc), backup schedule, product type, configuration info, volume configuration info, share info, Linux user info and warning configuration info. You can perform restore if necessary, and then rebuild a new console via the console info exported.

The functions of self-backup include: 1. Manually back up console database, scheduled job and configuration info; 2. Manually restore the console to certain

backup timepoint; 3. Directly export configuration info to a new console.

◆ **Self-backup Property**

In [Self-backup Property], you can configure save path, perform backup, etc.

➢ Click [Save Path] and click [Browse] to select the path to save. Then click [OK] to save configuration.

➢ Click [Backup] and enter the remarks of this backup, and then [OK] to back up console info to the save path configured.

◆ **Backup Package List**

[Backup Package List] lists all backup packages for the console under the current path.

➢ Select the backup package and click [Restore Console]. Enter the comments for this restore and click [OK] to restore the package to current console.

➢ Click [Delete] to delete the selected backup package.

◆ **Backup History**

[Backup History] displays the self-backup history. Click [Export] and you can save the information.

◆ **Restore History**

[Restore History] displays the history info of console restore.

5.11 Log Management

In "Log", AnyBackup Appliance provides client, user, system, access, RAID, update and VM logs for you to check the device status. Log records the backup or restore events, warning, errors, etc. By checking these logs, you can track operations or diagnose the reasons for failure.

5.11.1 Log Type

◆ **Client Log**

Enter "Client Log" and select the client in "Client List" to check the logs of this client.

◆ **User Log**

Enter "User Log" and you can check the operations of the user, such as the logs of password modification, email modification, etc.

◆ **System Log**

Log in by using an admin account and you can see the logs of system configurations in "Log Management".

◆ **Access Log**

Enter "Access Log" and you can see the access log via FTP, CIFS, NFS and iSCSI protocol, including access time, access directory, host name and IP.

◆ **RAID Log**

Enter "RAID Log" and you can check the RAID status of backup devices, including logs of RAID operation, volume operation and RAID status changing.

◆ **Update Log**

Log in by using the admin account and enter "Update Log". You can check the update logs including type, event, update time, descriptions, etc.

5.11.2 Log Content

It usually contains:

➢ Type: Include Error, Warning and Info.

➢ Time: Execution date and local time of the log.

➢ Event: Operation type, such as login, management, backup, restore, etc.

➢ Description: Details about the log.

5.11.3 Log Management

◆ **Export Log**

Select a log and click [Export] to save the log locally in text form.

◆ **Delete Log**

Select the log to be deleted and then click [Delete]. Click [Delete All] and you can delete all logs.

🔔 **Note:** Audit admin can view the log information of all users, as well as that of admin. However, admin cannot view the logs of audit admin.

Chapter 6 Backup and Restore

After successful deployment and configuration, you can log in to the console via the user account created by an administrator, thus performing backup and restore for data on the authorized client.

6.1 Backup Management

6.1.1 Overview

Backup management includes "Regular Backup" and "Backup Strategy". Click "Backup and Restore/Backup" to enter the corresponding window.

In "Regular Backup", you can create backup jobs, configure options, delete unnecessary backup jobs, etc.

In "Backup Schedule", you can create new strategies for groups, or modify/delete the strategies of certain groups. In addition, you can create/modify/delete strategies for one backup job.
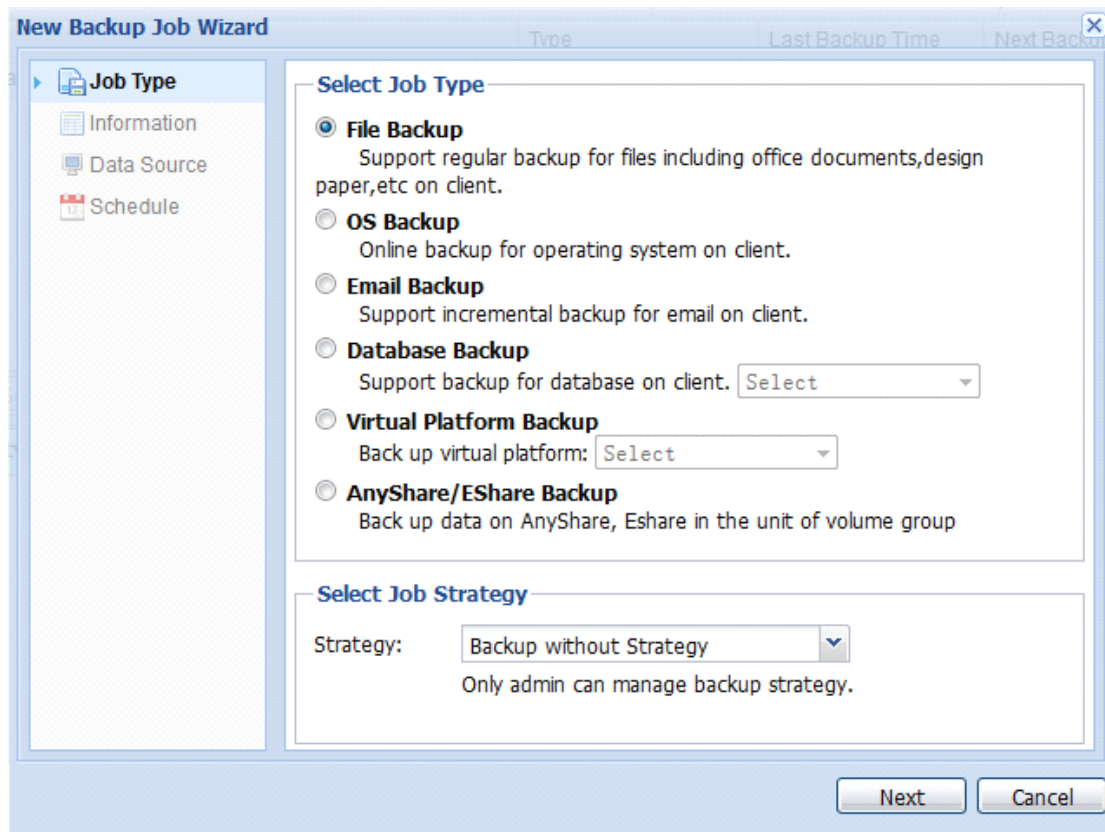
6.1.2 Regular Backup
6.1.2.1 New Job

Step 1: If you want to create a backup job for a database, you need to configure client as the database supported first. For detailed information, please refer to 5.2.2 Configure Client.

Step 2: Click [New] in "Regular Backup" and select the job type in "Job Type". Then configure backup strategy and click [Next] to continue.

➢ If "File Backup" of "Operating System Backup" is selected, select the job strategy in "Strategy".

➢ If "Database Backup" is selected, select the database type in the drop-down menu which includes SQL Server, Exchange Server, Oracle, Sybase, Active Directory, etc.

Figure 51 Select Job Type

Step 3: Configure job name, job group, destination, data deduplication, data source selection mode and data type in [Information]. Then click [Next] to continue.

Figure 52 Job Information

➢ Click "Dual-HA Binding" and you can bind dual-HA in [Dual HA/Cluster]. Then return to [Information] and select shared data on Dual-HA server.

➢ Click [Cluster Binding] and you can bind cluster in [Dual HA/Cluster]. Then return to [Information] and select shared data on cluster server.

Step 4: Select the client to be backed up in [Data Source]. Then unfold and select data source and click [Next].
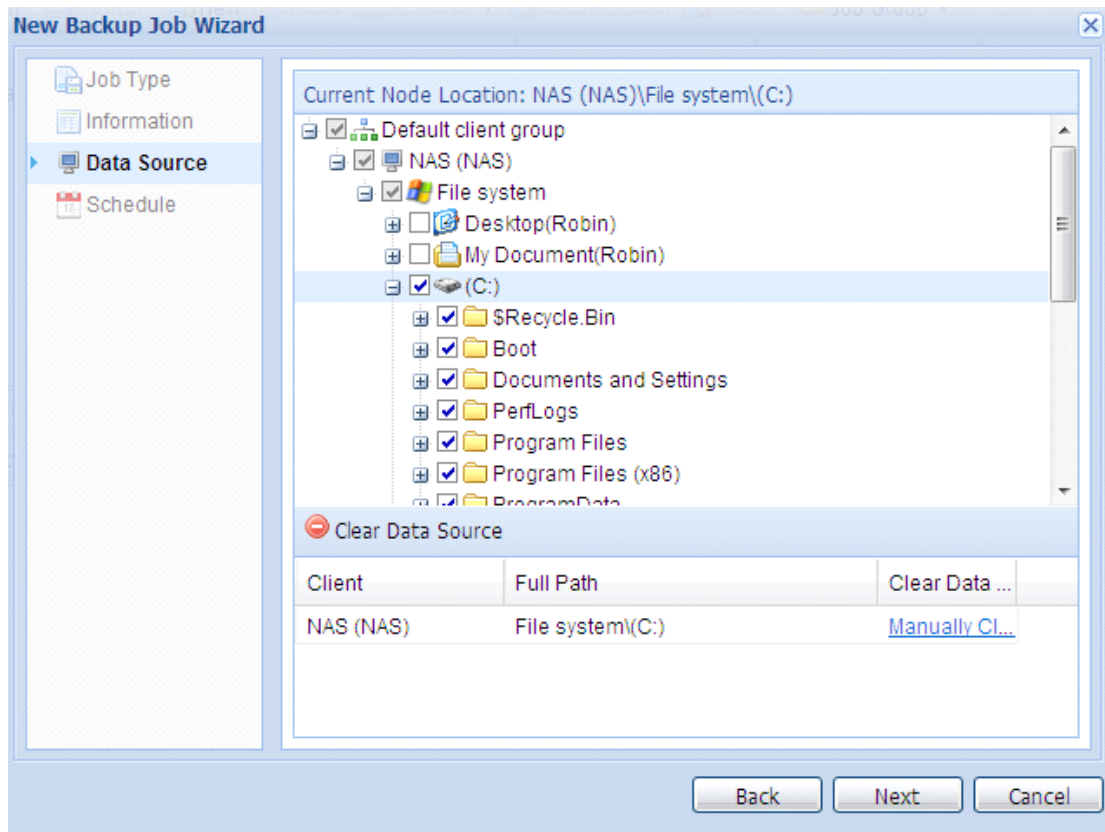
Figure 53 Select data source

Step 5: Click [Add] in [Schedule/Event] to display the [New Backup Schedule Wizard]. Enter [Schedule Type] to select execution frequency of Daily, Weekly, Monthly, Once and Event Trigger. For a detailed introduction, please refer to 6.1.2.2 Job Schedule. Then click [Next] to continue.

Step 6: Click [Schedule Content] to configure backup type, backup time and interval. You can also configure [Repeat Backup] in [Advanced Schedule Options], and then click [Done] to save the configuration.

Step 7: Backup to [Schedule/Event] to configure a full copy to retain. It is defaulted to 2 and can be positive integer between 0 and 10000.
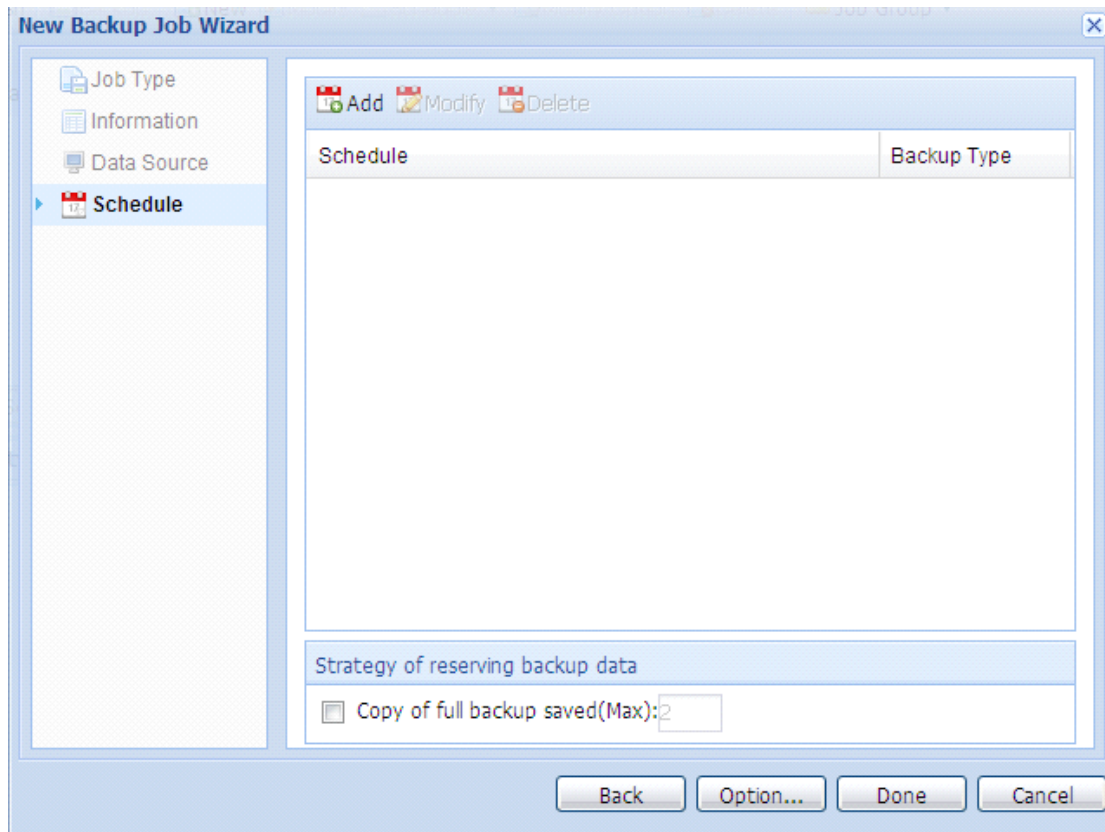
Figure 54 Configure Schedule/Event

Click [Option] on the right bottom of [Schedule/Event] to configure file filter, media options, advanced options, etc. For detailed information, please refer to 6.1.2.3 Job Options.

Step 8: In [Execute XX Backup] window dialog, you can select the backup type in [Backup Type] and enter the remarks below. Click [OK] to submit the job to execution queue, and then the [Job starts to back up] message will appear. If you want to view its execution progress, click [Execution].
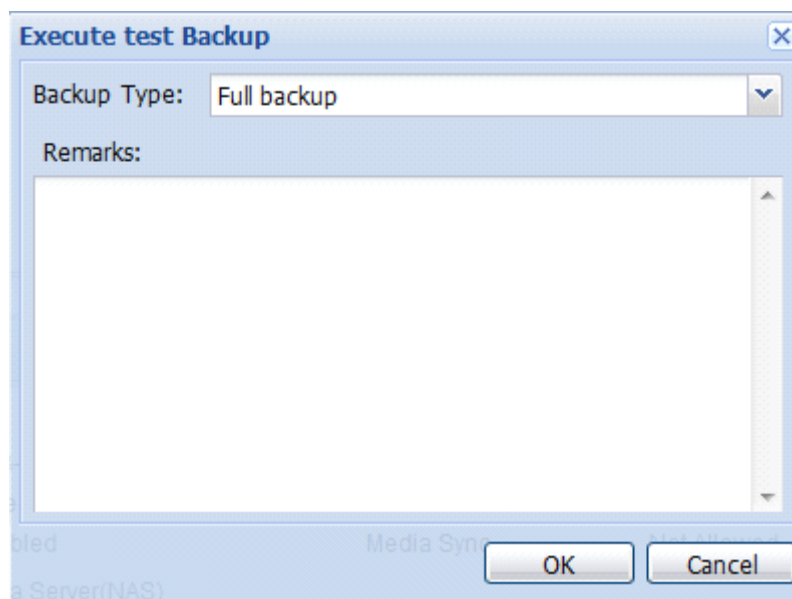
◆ **Backup**

Select the backup job created and click [Backup]. Then you can select backup time and add remarks. Click [OK] to finish operation.

◆ **Modify Job**

After job creation, you can modify in [Backup].

➢ Select the job to be modified and click [Modify].

➢ Click [Option] to modify the options of this job, and click [Schedule] to modify the schedules.

◆ **Delete Job**

Select the job to be deleted and click [Delete]. Select [Yes] in the confirmation window and all configurations of this job will be deleted.

◆ **Job Group Management**

Click [Job Group] and you can [Create], [Modify] and [Delete].

➢ Click [New] and enter group name and description in [New Group Info]. Additionally, you can change the group ownership of members by clicking "<<" or ">>". Then click [OK] to finish group creation.
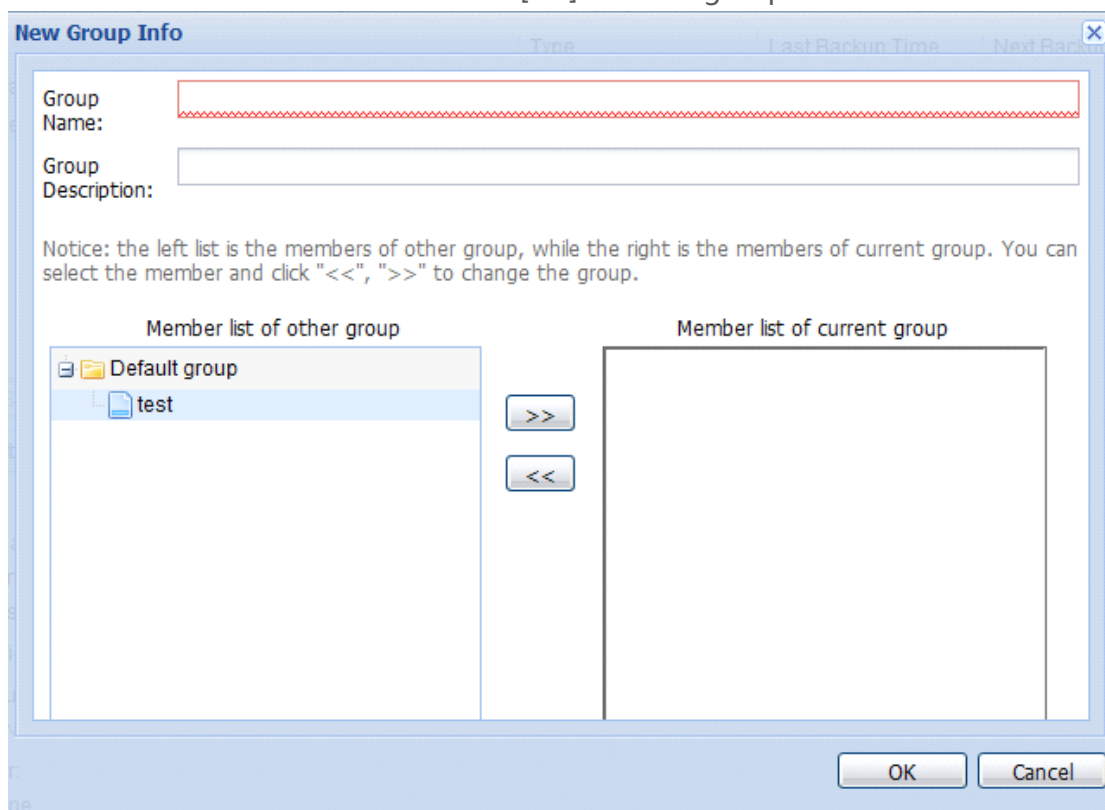
Figure 56 New group information

➢ Select the job group to be modified and click [Modify]. Enter group name and description and change the group ownership of members by clicking "<<" or ">>". Then click [OK] to finish group modification.

> ➢ Select the job group to be modified and click [Delete]. Select [Yes] in the confirmation window to finish group deletion. The members of this group will be moved to the default group.

6.1.2.2 Job Schedule

◆ **Add Schedule**

Select any backup job or backup strategy, and click "Modify Schedule" in the drop-down menu of [Schedule] to show the following:
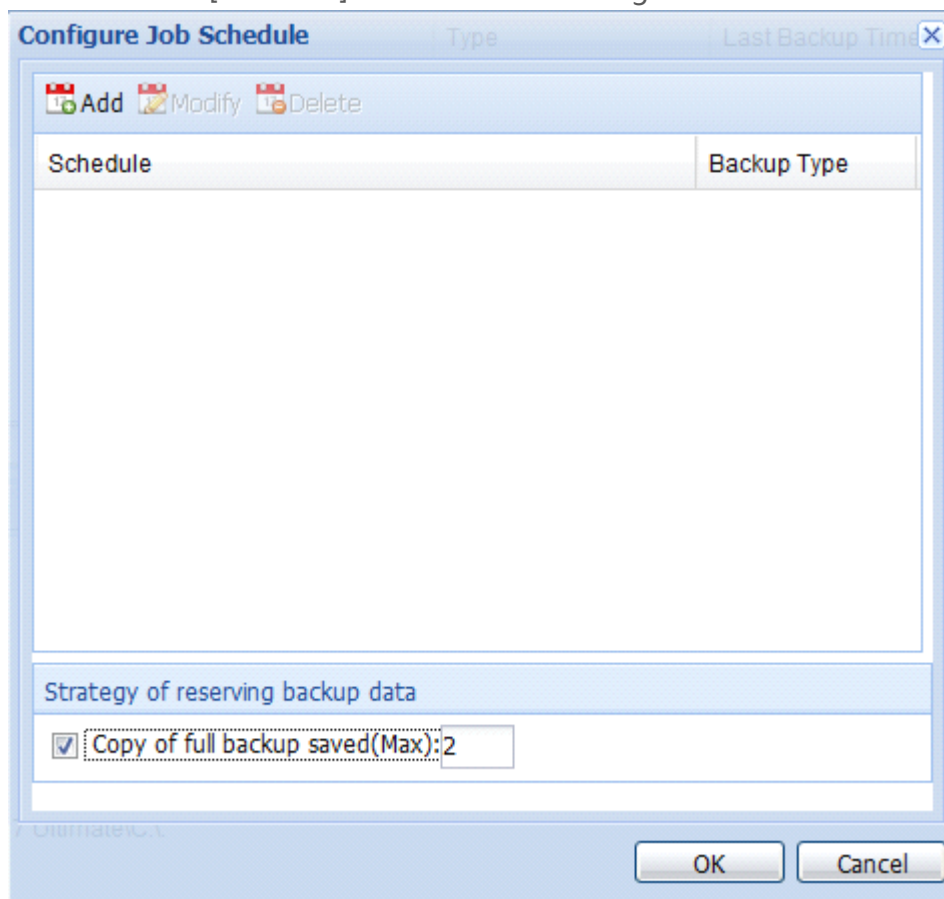
Figure 57 Configure Job Schedule

Click [Add] to display [Job Schedule Wizard] to configure execution frequency as Daily, Weekly, Monthly or Once. Then click [Next] to continue.
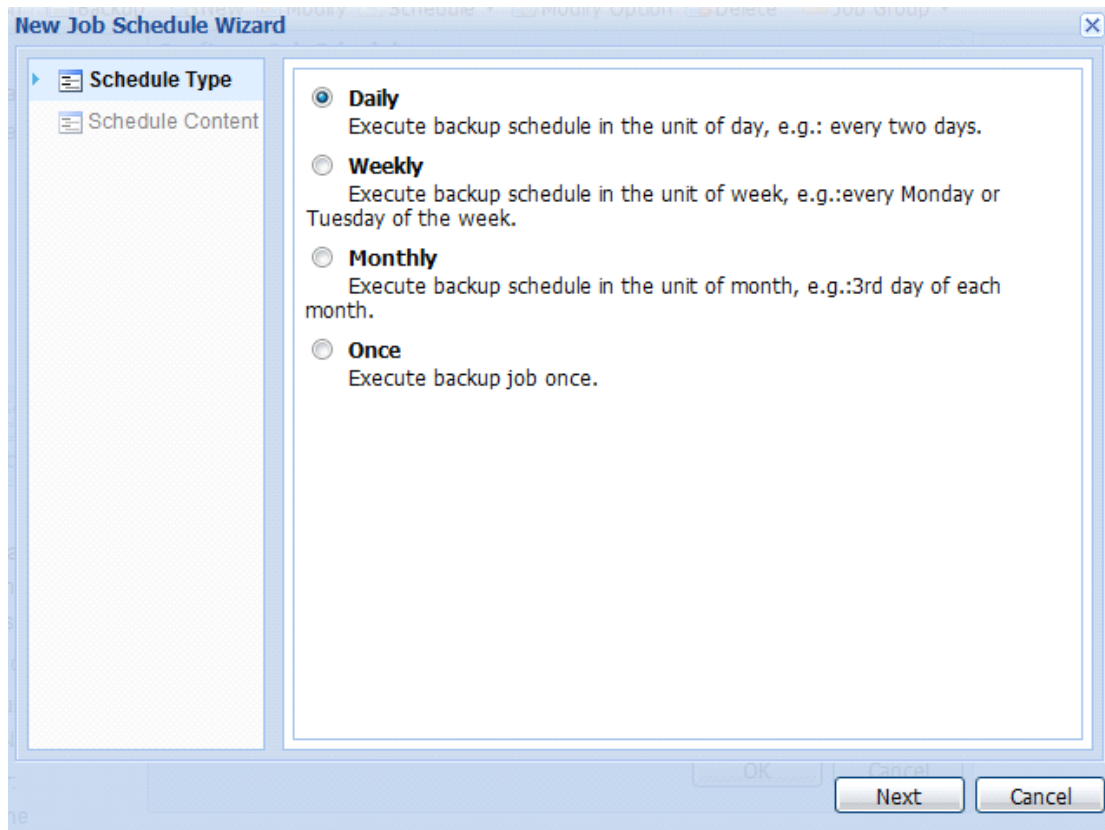
Figure 58 Select schedule type

Click [Schedule Content] to configure backup type, backup time and interval. You can also configure [Repeat Backup] in [Advanced Schedule Options], and then click [Done] to save the configuration.
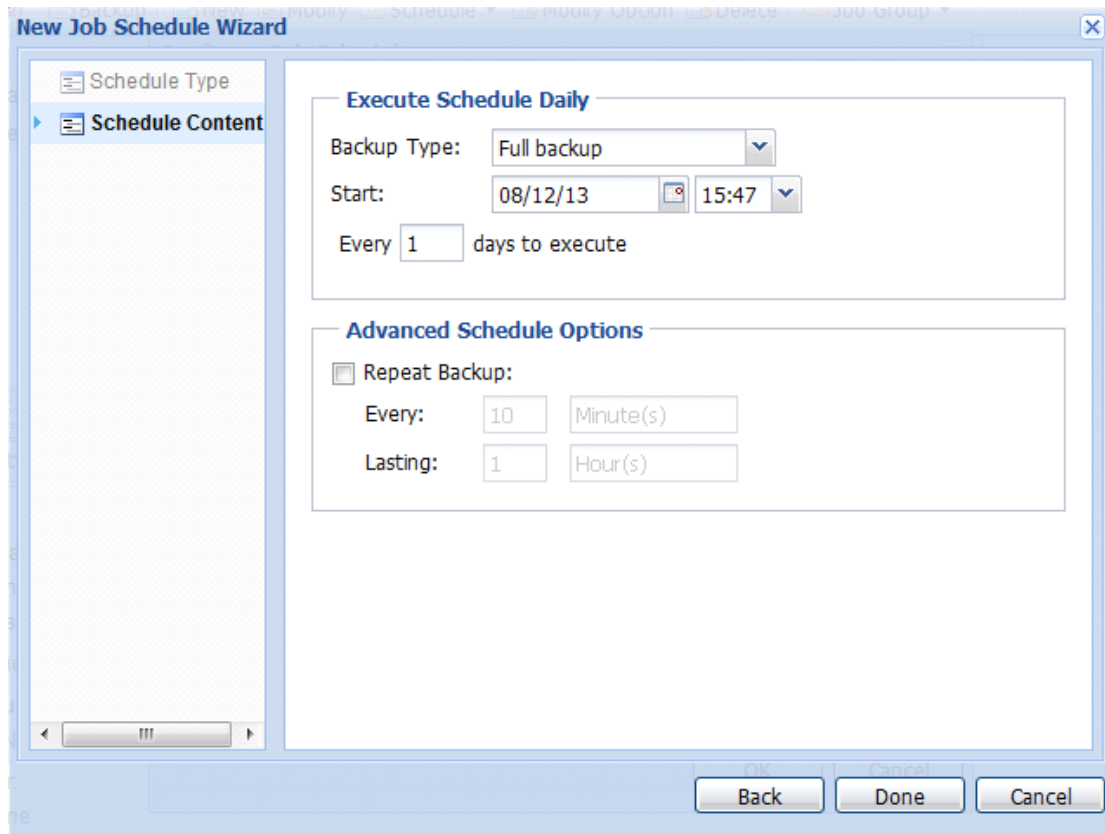
Figure 59 Configure schedule

◆ **Schedule Management**

Schedule can be modified and deleted after backup job or schedule is created.

➢ Click "Modify" in the drop-down menu of [Schedule] to modify job and full copies retained. Click [OK] to save modification.

➢ Click Pause" in the drop-down menu of [Schedule] to pause the schedule.

➢ Click "Resume" in the drop-down menu of [Schedule] to resume the paused schedule.

➢ Click "Delete" in the drop-down menu of [Schedule] to delete the schedule.

6.1.2.3 Job Options

◆ **File Filter**

The powerful file filter function of AnyBackup can exclude or contain only files of specified type, specified file name, specified directory, helping you to save storage space and accelerating backup speed.

Click [Modify Option] in [Backup and Restore].

➢ Click [File Filter] in [Job Options].
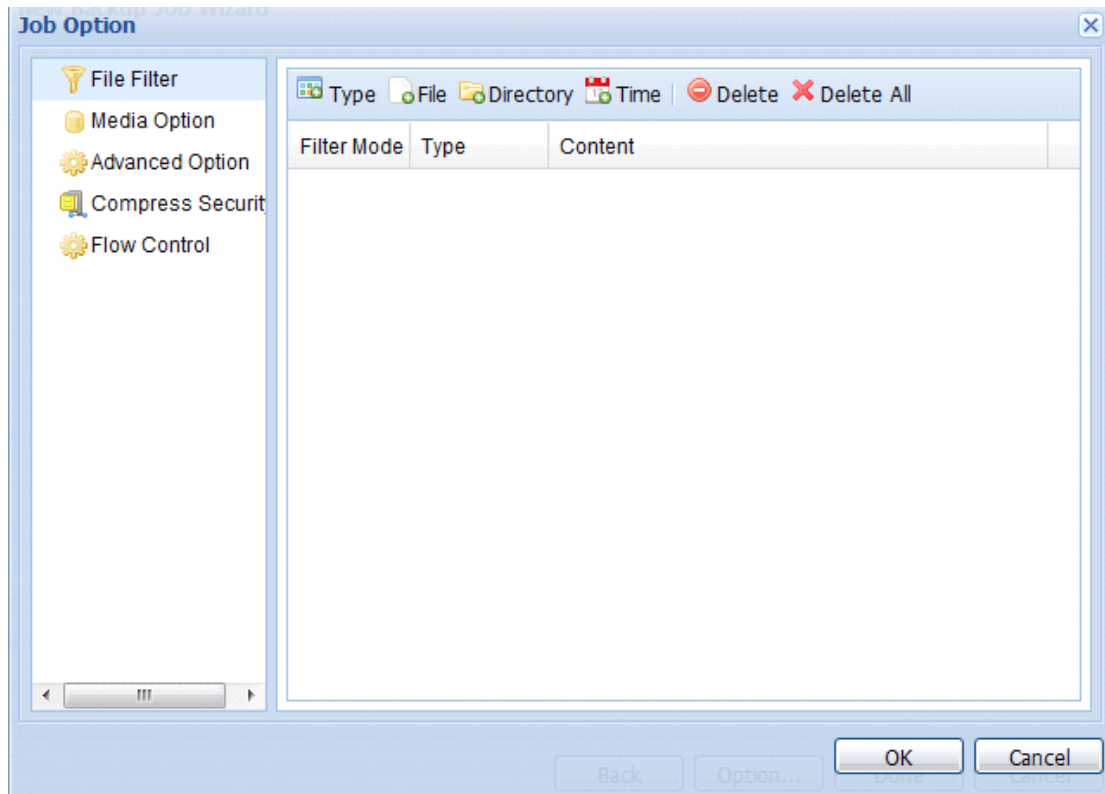
Figure 60 File Filter

- **Filter Type**: Click [Filter Type] to select to contain only or exclude, and then system file types in [Common Types] or enter extension manually in [Other File Types]. Click [OK] to save configuration.
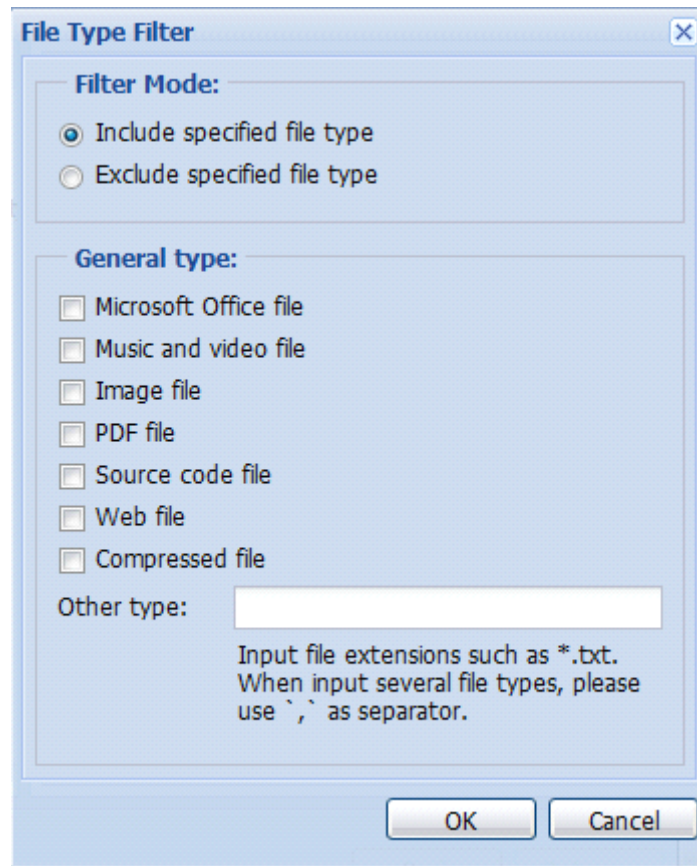
Figure 61 Filter Type

■ **Filter File**: Click [Filter File] to select to contain only or exclude. Then enter the file name and click [OK] to save configuration.
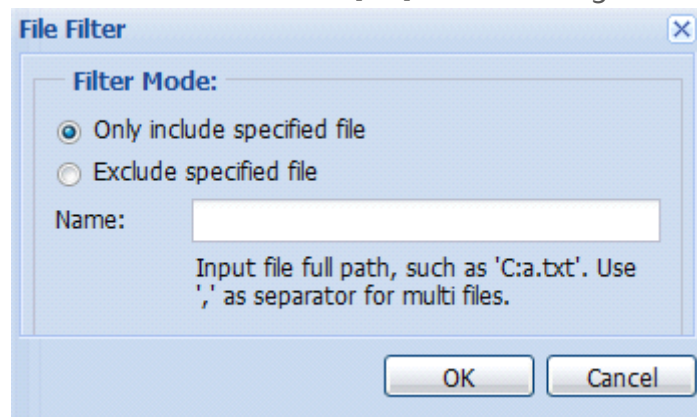
Figure 62 Filter File

■ **Filter Directory**: Click [Filter Directory] to select to contain only or exclude. Then enter the directory name and click [OK] to save configuration.
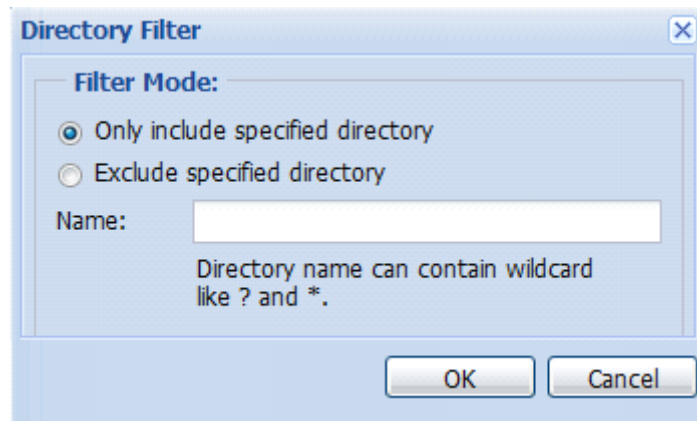
Figure 63 Filter Directory

- **Filter Time**: Click [Filter Time] to select to contain only or exclude. Then enter the filter time and click [OK] to save configuration.
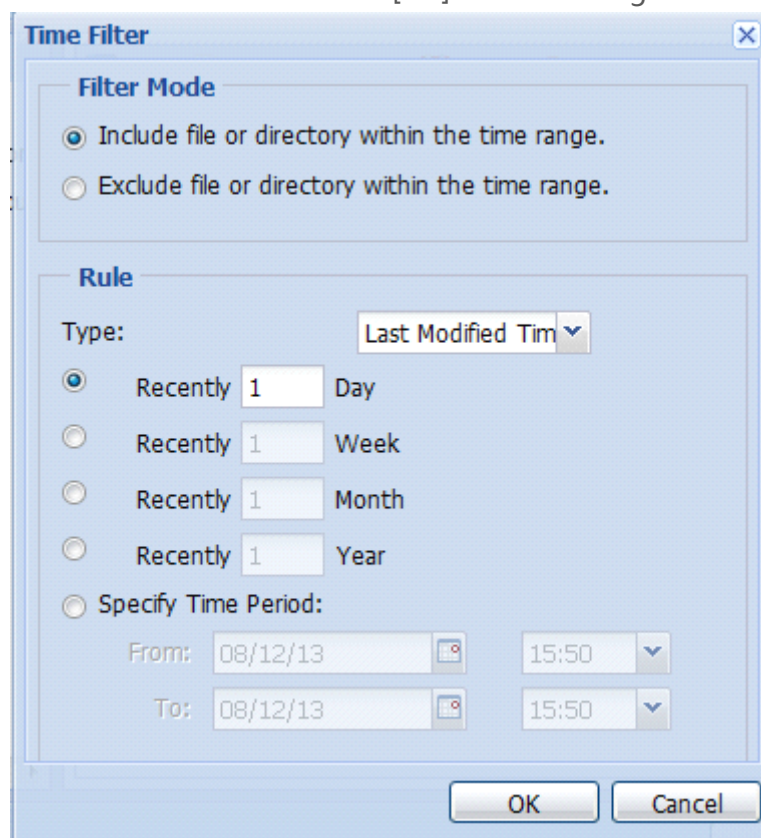
Figure 64 Filter Time

- **Delete Filter Item**: Click the filter item to be deleted and click [Delete]. Then click [OK] to finish. If you want to delete all filter items, click [Delete All].

◆ **Media Options**

By "Media Options", you can configure whether to allow media synchronization for the data of backup job, and you can also configure the max full copies retained for sync server.
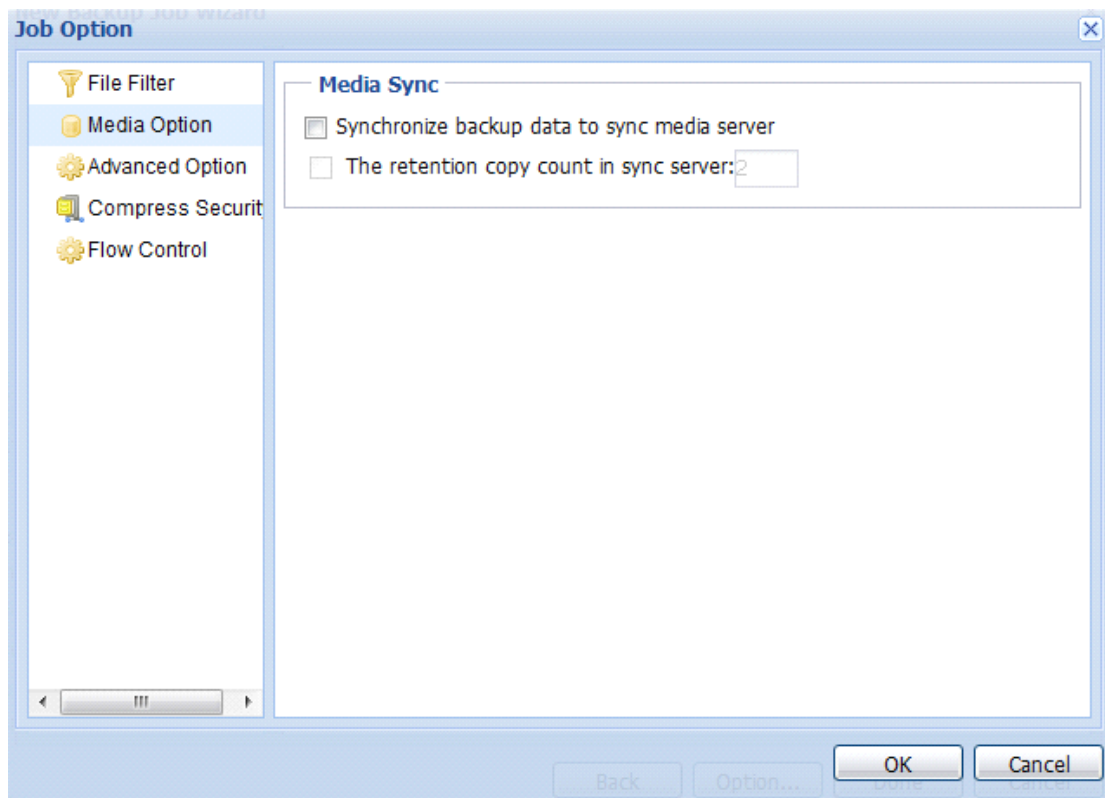
Figure 65 Media Option

➢ Mark "Allow to synchronize backup data to media sync server" to enable synchronization function.

➢ When synchronization function is enabled, the maximum full copy count can be configured.

◆ **Advanced Options**

By "Advanced Options", you can configure a custom script, which includes:

➢ Script executed before backup

➢ Script executed after restore

ð Note: The script entered here requires an absolute path.
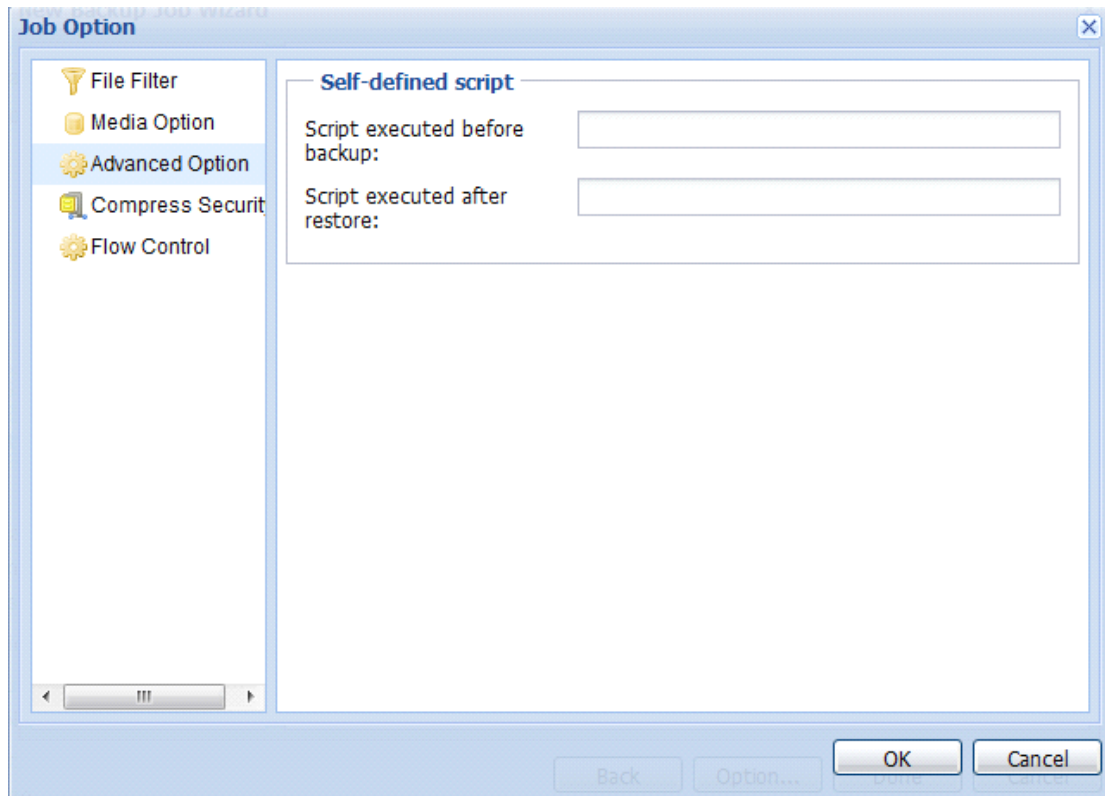
Figure 66 Advanced Options

◆ **Compression and Encryption**

AnyBackup Appliance supports data compression before transferring to media server and storing in file of OFS system, thus backup speed is enhanced and data space is reduced. Furthermore, data encryption is also supported to ensure data security.

The default configuration of compression is "disabled" and encryption is also "disabled". When compression and encryption is enabled, you can configure CPU resource count between 1 and 6 (default by 1). If the count configured exceeds the actually available count, it will change to the available one automatically.

If both compression and encryption are enabled, first encryption and then compression during backup, but first decryption and then decompression during restore.
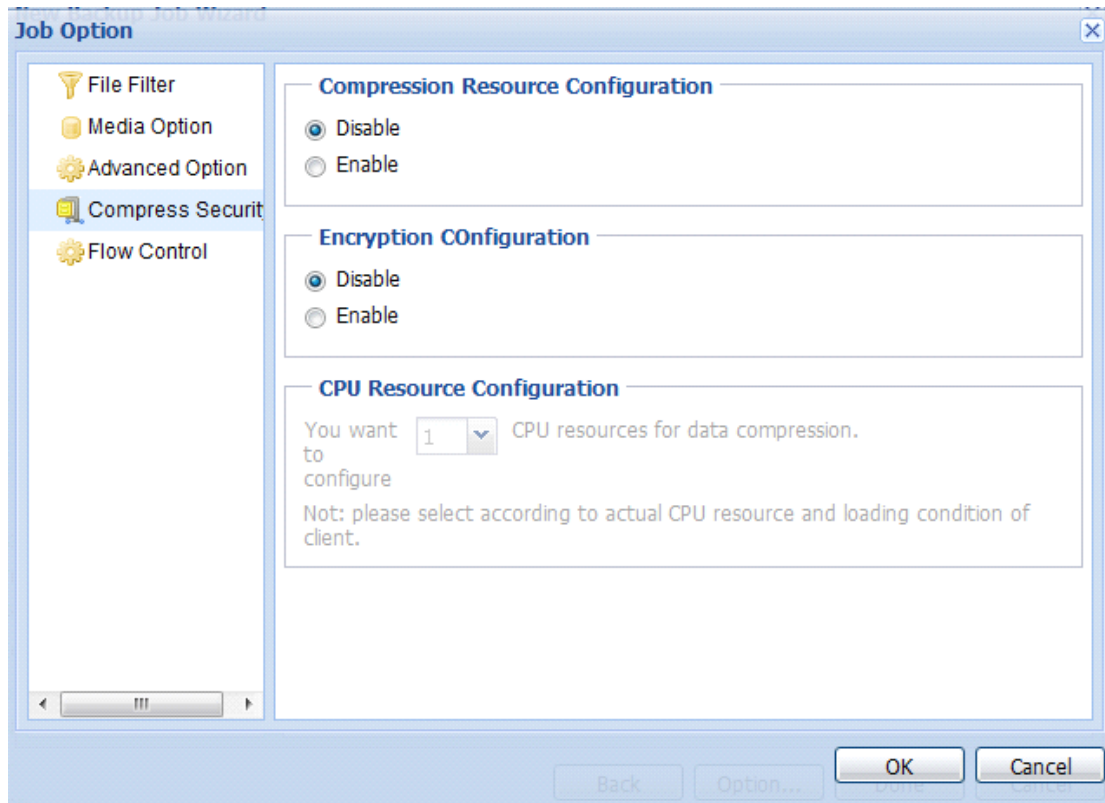
Figure 67 Data Compression

◆ **Flow Control**

Flow control is a backup job strategy to reduce the impact on business bandwidth.
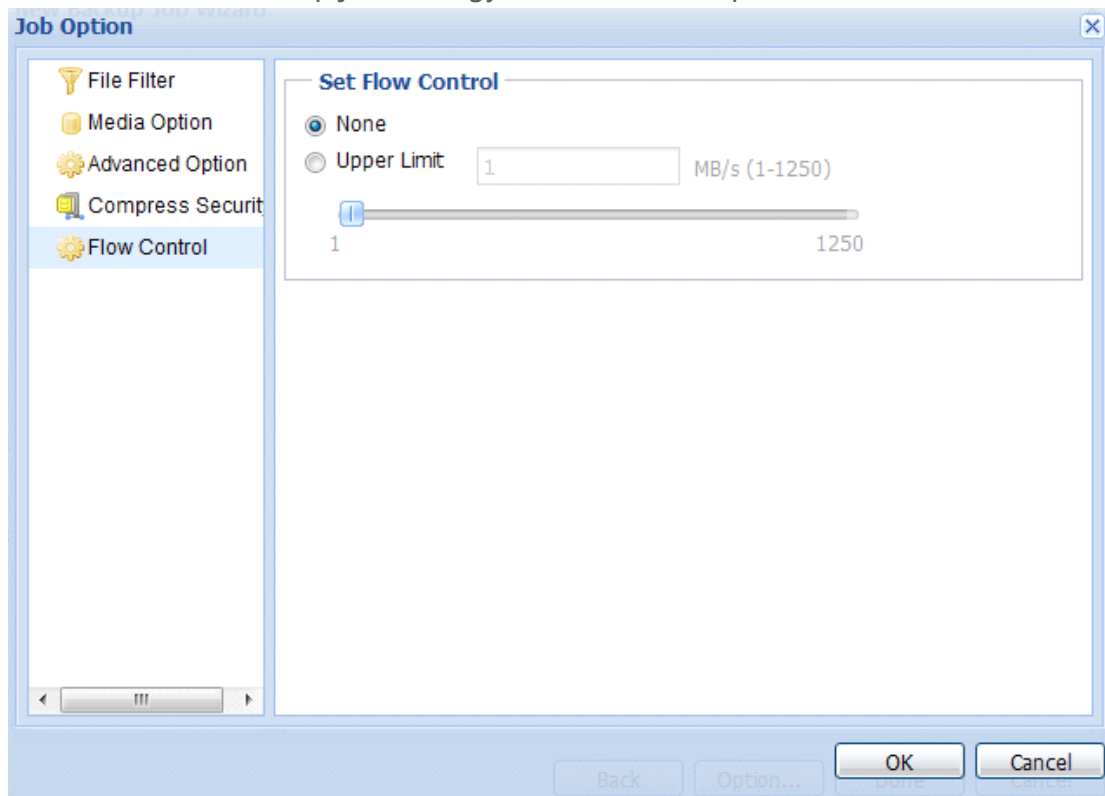
Figure 68 Flow Control

> Flow control takes effect for backup job only. It does not limit the speed of restore job.

> Flow control can perform during a single backup job. There is no impact among jobs.

> Flow control will take effect in the next backup after it is configured. It does not take effect for the current executing job,

> If LAN-FREE is enabled, flow control cannot be enabled.

6.1.3 Backup Strategy Management

Click "Backup and Restore/Backup/Backup Strategy" to display the related dialog box.

◆ **Create Strategy**

Step 1: Click [New Strategy] in [Backup Strategy] to select strategy type which includes "File Backup Strategy" and "OS Backup Strategy". Then click [Next] to continue.
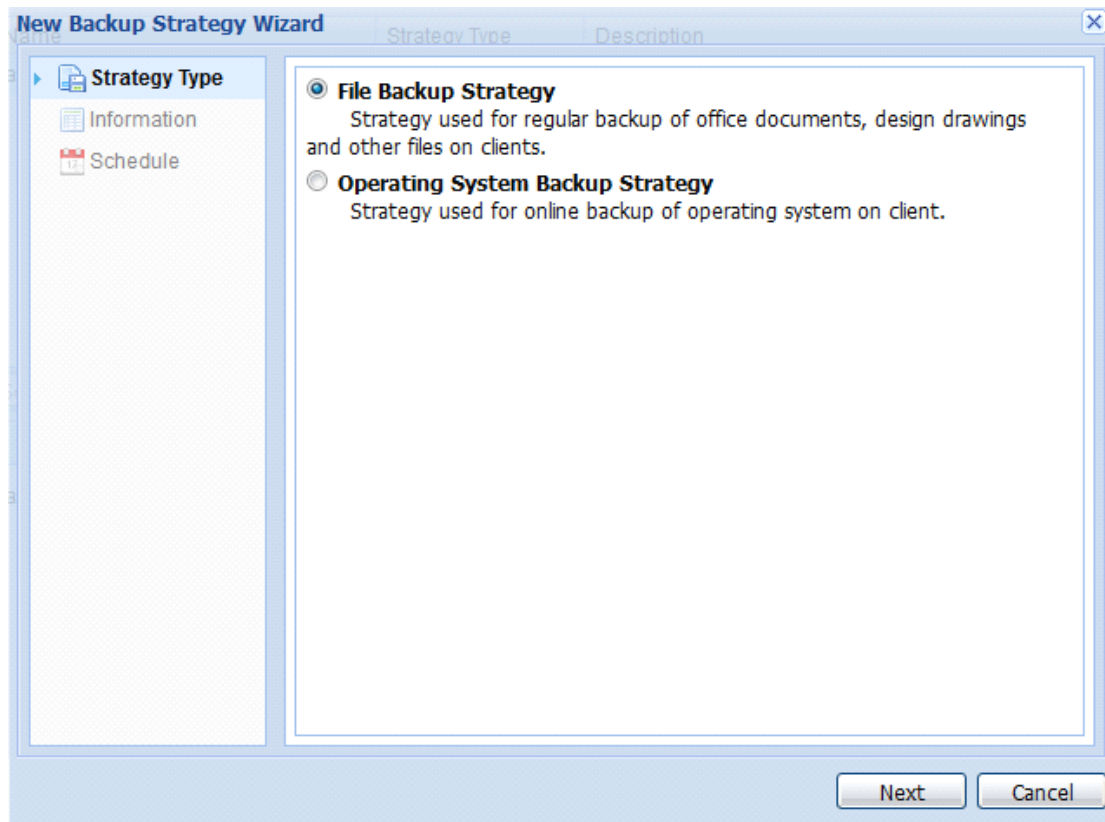
Figure 69 Select strategy type

Step 2: Enter strategy name, strategy group and backup destination in [Information] and click [Next].

Figure 70 Basic information of strategy

Step 3: Click [Add] in [Schedule/Event] to select schedule type, configure schedule content and then click [Done].

Step 4: You can also click [Option] in the bottom-right to configure file filter, media options and data compression.

◆ **Modify Strategy**

Select the strategy to be modified and click [Modify] to modify strategy name, strategy group and description.

◆ **Delete Strategy**

Select the strategy to be deleted and click [Delete]. Click [Yes] to finish deletion.

◆ **Strategy Group Management**

Strategies can be added to strategy group for unified management.

Strategy group management includes creation, modification and deletion. For detailed information, please refer to "Backup Management/Job Group Management".

6.2 Restore Management

AnyBackup Appliance provides browse to restore to help you restore data promptly and accurately.

◆ **Notice for Deployment**

  ➢ If browse to restore is to be performed, install client on the client machine to be restored.

◆ **Notice for Restore**

  Browse to Restore

  ➢ The target volume of browse to restore should be larger than the total space of source volume, otherwise the restore will fail.

  ➢ In browse to restore volume replication data, the current data of the target volume on the client selected will be cleaned up, please select target volume carefully.

  ➢ In restore, target volume cannot be accessed if it is powered down.

  ➢ In restore, deletion of the volume being restored is not allowed.

  ➢ If multiple volumes of one job are selected for browse to restore, it can be restored to original path only. If you want to restore to another location (local or remote), please select respectively.

  ➢ In browse to restore for database, data can be restored to local or the original path of remote only.

  ➢ In hetero-machine restore for database, the installation path and storage path must be the same.

6.2.1 Browse to Restore

AnyBackup Appliance supports restoring backup data to specified and authorized client.

  ➢ Click "Backup and Restore/Restore/Browse to Restore".

  ➢ Select the client of backup data to be restored in [Client List].

  ➢ Select the timepoint to be restored to in the drop-down menu of [Timepoint] which is defaulted to the initial backup timepoint of the job.

  ➢ Click [Backup Job] in [Backup Data] to select the backup job, and then unfold the job.

  ➢ Select the backup data and timepoint and then click [Restore to Client].

  ➢ Select the client to be restored to in the drop-down menu of [Restore to Client].

  ➢ Then click [Restore] to submit to execution queue.

  ➢ The message of "Current restore request has been submitted to execution queue, execution item name is XXX" will display. If you want to view the execution progress, click [Execution] to check.

6.3 Execution Management

Log in to the management console and click "Backup and Restore/Execution" to switch to related window. Here you can check the job queue executing and historical records.

6.3.1 Routine Execution

It organizes the jobs executing and to be executed in the way of queue, and meanwhile displays information such as job name, OS type and running status.

◆ **Refresh**

Click [Refresh] to automatically refresh the latest execution status.

◆ **Stop Execution**

Click [Execution] to stop the executing job selected.

◆ **Stop All**

Click [Stop] to stop all the executing jobs.

◆ **Filter**

Click [Filter] to configure the job types displayed in job list of routine execution.

➢ Type Filter: Filter according to job types, which include full backup, restore, reverse direction media synchronization, etc.

➢ Other Filters: Filter according to job status, such as waiting, running, etc.

◆ **Output Information**

Click "Output Info" to show job status, warning of each executive, error info and execution time.

◆ **Execution Details**

Click "Execution Details" to display the executive name and current status.

6.3.2 Continuous Execution Job

Continuous execution job lists the information of all media synchronization.

◆ **Refresh**

Click [Refresh] to refresh the current status automatically.

◆ **Start**

Click [Start] to change to running status from pause or stop.

◆ **Stop**

Click [Stop] to change to stop status from running or pause.

◆ **Pause Interval**

Select one media sync job and click [Pause Interval] to configure pause period daily, weekly or monthly.

➢ Click [Add] to display the dialog box of "Add Pause Interval". Three options are provided in the drop-down menu, namely daily, weekly and monthly.

- Daily: the pause interval configured takes effect every day.
- Weekly: the pause interval configured takes effect every week.
- Monthly: the pause interval configured takes effect every month.
- Click [Modify] to modify pause interval.
- Select the time interval and click [Delete] to finish deletion.

◆ **Auto Cleanup**
- Select the continuous execution job and click [Auto Cleanup] to configure the cleanup time of output information.
- The retention time of output information includes 1 day, 2 days, 1 week, 2weeks and 1 month (1 week by default).
- Click [OK] to save.

◆ **Filter**

Click [Filter] to configure the job types displayed in job list of continuous execution.
- Type Filter: Filter according to job types, which include media synchronization, replication, disaster recovery, etc.
- Other Filters: Filter according to job status, such as running, pausing, stopping, etc.

◆ **Output Information**

Click "Output Info" to show job start, pause, stop, warning of each executive, error information and execution time.

◆ **Execution Details**

Click "Execution Details" to display the executive name, status and remarks.

6.3.3 Historical List

Historical list is to show the executed job and its type, result and time. Output information and report are also displayed.

◆ **Refresh**

Click [Refresh] to view the latest historical list.

◆ **Delete**

Click [Delete] to delete the current historical list.

◆ **Delete All**

Click [Delete All] to delete all historical lists.

◆ **Export**

Click [Export] to export the execution list for users to download.

◆ **Filter**
- Click [Type Filter] to select filter type which includes all, backup, restore, reverse direction media synchronization, etc.
- Click [Other Filters] to select all, succeeded, succeeded but with warnings, failed, etc.

◆ **Name Filter**

Enter key words in the [Name Filter] and click search icon to filter.

◆ **Export Information**

Select the historical list of a job and its execution information can be viewed in [Export Info].

◆ **Report**

Select the historical list of a job and its execution result can be viewed in [Report]. Click the draw button before report to view the backup information of the time-point.

6.4 Regular Backup and Restore

6.4.1 Regular Backup and Restore for File System

◆ For detailed information of regular backup and restore for file system, please refer to 6.1.2 Regular Backup.

◆ For detailed information of restore, please refer to 6.2.1 Browse to Restore.

6.4.2 Regular Backup and Restore for System
6.4.2.1 Regular Backup and Restore for Windows

Step 1: Log in to the management console and click "Backup and Restore/Backup/Regular Backup".

Step 2: Click [New Job] to select [Operating System Backup] in [Job Type]. Then click [Next] to continue.

Step 3: Enter job name, select job group, destination, data source selection mode, data type, and click [Next].

Step 4: Mark the operating system to be backed up in [Data Source] where available clients are displayed, and then click [Next].
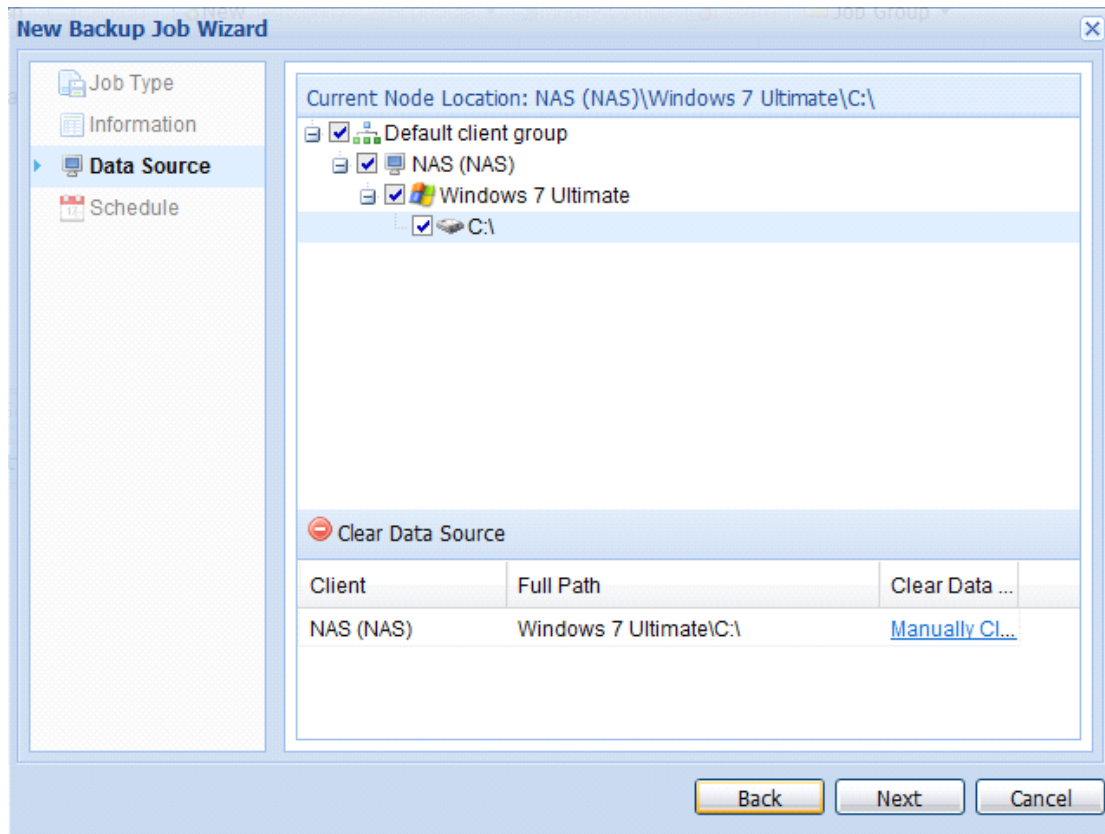
Figure 71 Select Data Source

Step 5: Enter [Schedule/Event] to configure detailed job schedule via "add, modify, delete". When configuring [Start Time], try to back up when server is free. Furthermore, when configuring [Retention Strategy], consider your storage space and data demands.

Step 6: You can configure file filter, media option, compression/encryption and flow control in [Options] and click [OK] to finish creation.

◆ **Windows System Restore**
Step 1: Boot SRE
  ➢ For normal boot of SRE, please configure the start option of BIOS correctly.
  ➢ The initial interface of SRE is as follows:

Step 2: Configure RAID/Disk Control Drive
  ➢ For successful system restore, drive of disk controller/RAID controller must be loaded correctly. Currently, most mainstream drives of disk controller/RAID controller are supported.

- For situations of boot via CD/ISO Image/USB, correct drive will be automatically loaded when it starts.
- SRE will load some basic disk drives by default when it starts, then the disk partition list recognized by current system will be displayed for about 5 seconds.

```
--------------------------
Below is partitions table
--------------------------
hda      4194304
hda1     200781
hda2     2963992
hda3     1028160
--------------------------
Press any key to config RAID/SCSI/SATA devices in 4 seconds.
```

Step 3: Select the disk to be restored
- When there are multiple disks, a dialog box will display for users to select which disk to be restored to. Click each disk and the detailed partition information will be displayed, such as partition name, type, size for users to judge and select a correct one.

Step 4: Configure local network
- Most mainstream Fast/10GB Ethernet are supported and it retrieves an IP by DHCP by default. If dynamic allocation of IP is not supported, please configure it manually.
- The recognized NIC device and IP address will be displayed in [Network]. In Linux system, NIC device is named by the form of eth0, eth1.... eth0 is the first NIC and eht1 is the second, and so on. Select the NIC to be configured and select the way to configure IP: auto or manual. Then click [Next].

Step 5: Configure console information
- Enter "Server Address", "Port" in "Configure Console Information" and select the login mode. Enter "Username" and "Password" and click next to connect to the server.
- "Server Address" is the IP of console and "Port" is 9900 by default. "Username" is the login user of console and "Password" is the password to log in console.

Step 6: Select the job to be restored and backup time-point
- After connecting to backup server successfully, it will switch to the page of job selection, which includes "Media Server" and "Media Sync Server". Select the media of backup data, unfold job to see the client list. Select the client to be restored to get related timepoint. Select one and click Next to start system restoration.

Step 7: Partition for disk

- ➢ At the beginning of system restore, SRE will parse whether the current disk partition information is consistent with that of system backup. If restoring to a new disk, or the partition information is inconsistent, it will prompt whether to partition.
- ➢ If partition is not selected, it will adopt the default partition for disk, or adopt the current partition format.
- ➢ If partition is selected, you can partition manually in the dialog box. It will inform you of the required partition count and minimum space for successful system restore, and these criteria must be satisfied.
- ➢ Create a new partition and space can be configured manually. Or you can select all free space left. The partition type should be consistent with that of the original system.
- ➢ Then click [OK] to create.

Step 8: Start system restore

- ➢ After configuration of partition, system restore starts. It will first format the disk partition according to partition and file system, and then restore the boot information and files in system later. The execution information of each stage will be displayed. Furthermore the file name being restored and its progress will be displayed as well.

Step 9: Restore I/O operation generated in backup.

- ➢ You can select "Yes" or "No". Under most circumstances, "No" will not affect the normal use of system. But when the system has problems, select "Yes" to restore the I/O operation in backup. By test, I/O backup and restore will enable to effectively support application of exchange, sql, Hyper-V, etc. so selecting "yes" is recommended here.

Step 10: Restore finished, boot system again

- ➢ After successful system restore, click "Yes" to restart the restored system.
- ➢ If restoring from CD or USB, please take the disk out or configure in BIOS the start sequence (Start from Hard Disk) to prevent SRE from starting again.

6.4.2.2 Regular Backup and Restore for Linux

◆ **Operation of Linux Backup**

Log in to the management console and click "Backup and Restore/ Backup/ Regular Backup".

Step 1: Click [New] to show the "New Backup Job Wizard" dialog.

Step 2: Select [Operating System Backup] and backup strategy in "Job Type". Click [Next] to continue.

Step 3: Enter job name, job group, destination in [Information] and click [Next].

Step 4: Select the data source to be backed up in "Data Source".
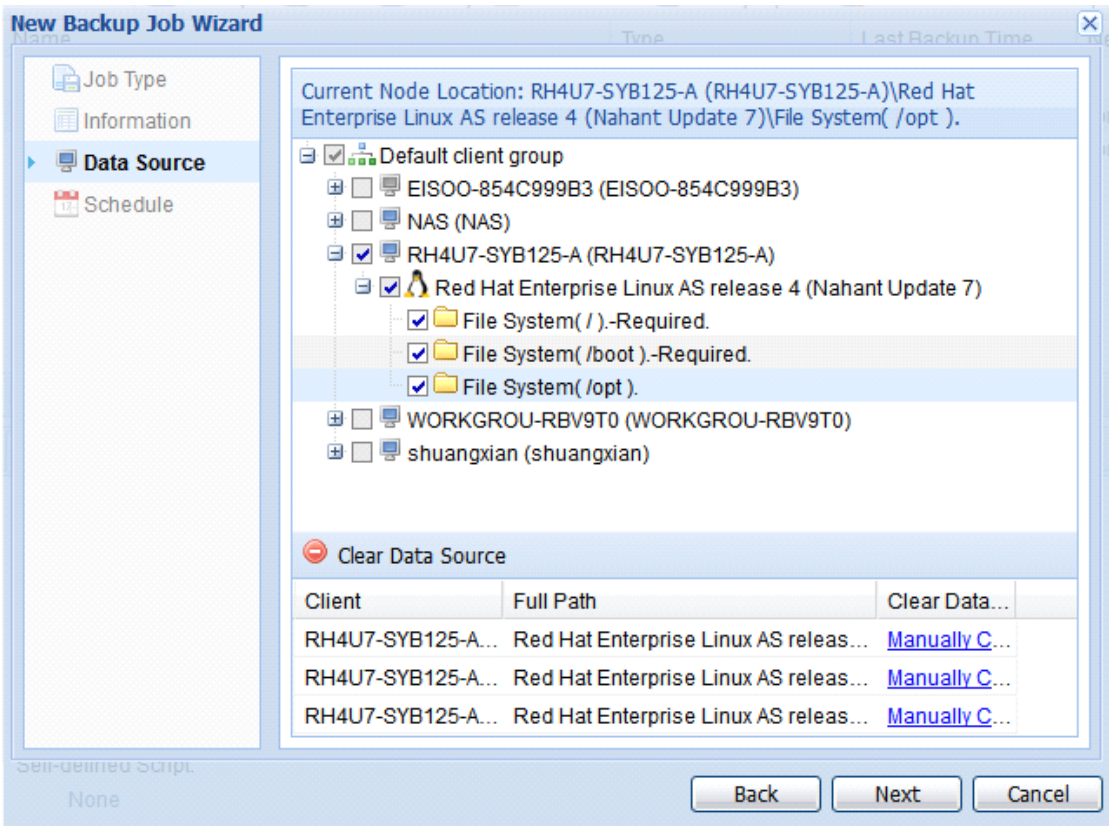
Figure 72 Select data source

Step 5: Enter "Schedule/Event" to add/modify/delete detailed schedule. Click [Option] to set compression, advanced option, etc. For detailed information, please refer to "Backup/Backup Strategy". Then click [Done] to finish.

Step 6: The "Execute Linux Backup" dialog box will show, you can add comments and click [OK] to start execution.

◆ **Operation of Linux Restore**
Please refer to Windows restore.

6.4.3 Backup and Restore for Email

◆ For detailed operation of email backup, please refer to 6.1.2 Regular Backup.
◆ For detailed restore, please refer to 6.2.1 Browse to Restore.

6.4.4 Backup and Restore for Database

6.4.4.1 Regular Backup and Restore for SQL Server

◆ **Function Overview**
As a database management system, Microsoft SQL Server features a graphical user

interface, which makes system management and database management easier and more intuitive. It also has rich programming interface tools, which provide more options for users to make programming. Fully integrated with Windows NT, SQL Server makes use of many functions of NT, such as sending and receiving massages, security for management of login, etc.

◆ **Backup Type**

There are three kinds of backup for SQL Server: full backup, differential backup and transaction log backup.

1. Full Backup

Full backup is backup for all data in database. Compared with transaction log backup and differential backup, it needs more storage space and requires more time but its operation frequency is lower.

2. Differential Backup

Differential backup takes the changed data after the latest full backup. Before restoring data of a differential backup, data of full backup must be restored first.

Compared with full backup, differential backup requires less storage space and backup time. Thus it can be used frequently to reduce the risk of data loss. It is especially effective for the same data modified several times.

Transaction log is a series of records for modifications and transactions in the database. Transaction log records the beginnings of each transaction.

One data file and one transaction log must be contained in SQL Server database. Data and transaction log information never mixes in a same file, and each file can be used by one database only. SQL Server restores transaction by transaction log of each database.

Use differential backup to restore data to the timepoint of differential backup. If you want to restore to the precise fault point, you must use transaction log backup.

◆ **Backup Wizard**

Configure Client

Log in to the Management Console as admin and click [System] > [Client] > [Configure], the [Modify Client Configuration] dialog will show. Then mark [SQL Server], and click [OK].

New Job

Step 1: Enter [Backup] and click [New] to show the dialog box of [New Backup Job Wizard]. Select [Database Backup/SQL Server] and click [Next].

Step 2: Enter job name, job group, destination and backup media. Common data source cannot be modified. Then click [Next] to continue.

Step 3: Mark database of whole instance of SQL Server in [Data Source] (Backup for all databases are recommended. Unnecessary databases can be removed if required). Click [Next].
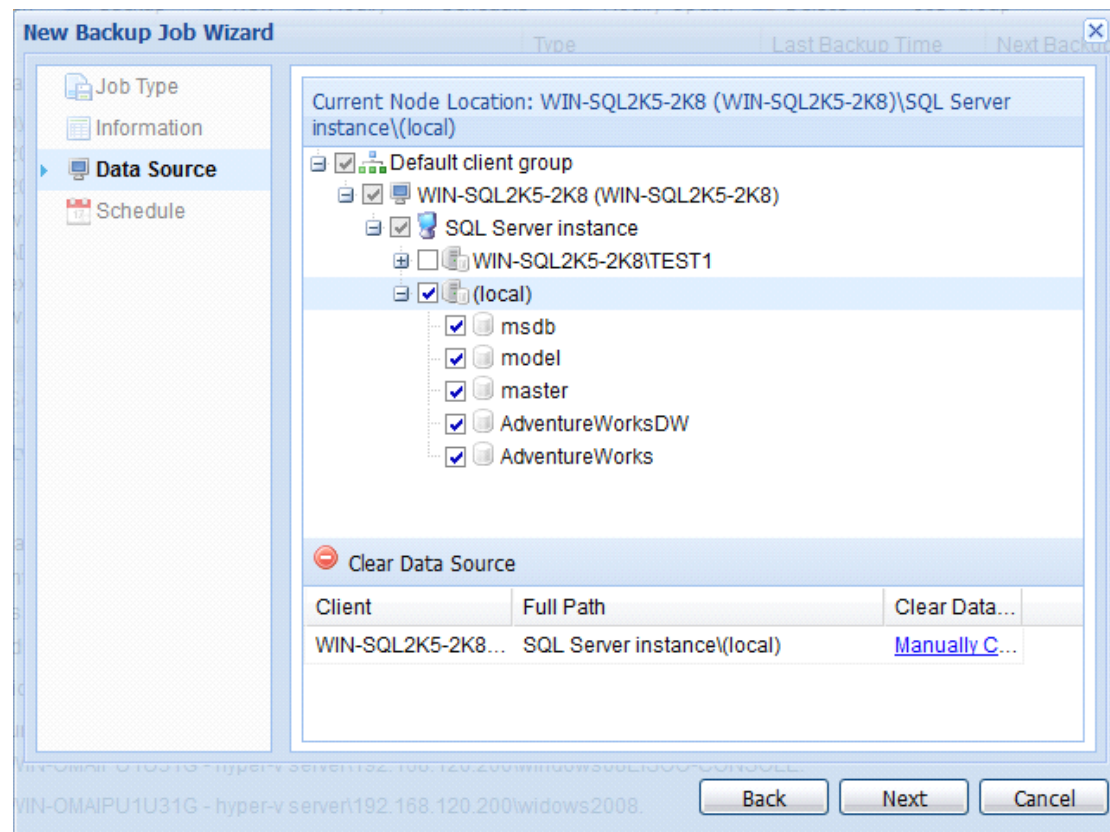

Figure 73 Select Data Source

 Note: Using one database in more than one job is not recommended, as it may cause errors.

Step 4 Enter [Schedule/Event] to configure detailed job schedule via "add, modify, delete". You can also configure media option, compression/encryption and flow control in [Options]. Click [OK] to finish creation.

➢ Data compression supports transferring data to media server after compression, and saving in OFS system file, thus enhancing backup speed and reducing the space occupied. Furthermore, data encryption is supported to ensure data security.

➢ The default compression and encryption configuration is "Disabled". When compression/encryption is enabled, CPU resource count, which is defaulted by 1, can be configured between 1 and 6 according to own

needs. If it exceeds the actual CPU resource count available, it will adjust automatically.

- ➢ Advanced compression compresses the data by the property parameter of SQL Server itself. It supports SQL Server 2008, 2008R2 and 2012.
- ➢ Standard compression compresses data by selecting appropriate CPU count based on actual CPU resource and loading condition. All versions are supported.
- ➢ Either or both forms of compression can be selected.

◆ **Configuration of Best Backup Strategy**

After selecting data source for backup, click [Next] to enter [Schedule/Event] where you can configure detailed job schedule by using "add, modify, delete" and configure media synchronization in [Options].

- ➢ SQL job schedule: Full backup every weekend + differential backup every day+ transaction log backup every N hours.
- ➢ The start time is recommended to be set at the time when the server is free.
- ➢ Save the data for 4 weeks (4 full copies), or it can be decided based on storage space and data storage time.

◆ **Restore Wizard**

Notice before Restore

- ➢ To restore a database to another Client, a database server which has the same instance name with the database in source Client needs to be installed in the target Client.
- ➢ When restoring master database, SQL Server service must be restarted in single user mode. After recovery, the service will be started in multi-user mode. Therefore, all other related database service except for SQL Server database service must be closed before restoration.
- ➢ If the database is being used during restore, restoration will fail.
- ➢ Make sure database is not connected by other applications during restore. Application connected with this database should be disconnected and enterprise manager should be closed.
- ➢ Hetero-restore requires the same instance name.

Operation of Restore

Step 1: Log in to the Management Console and click "Backup and Restore/Restore/" to switch to the page of browse to restore.

Step 2: Unfold the SQL Server job to be restored and select the client for restore.

Step 3: Click [Time Point] and select one time point. Then select the SQL Server database to be restored.
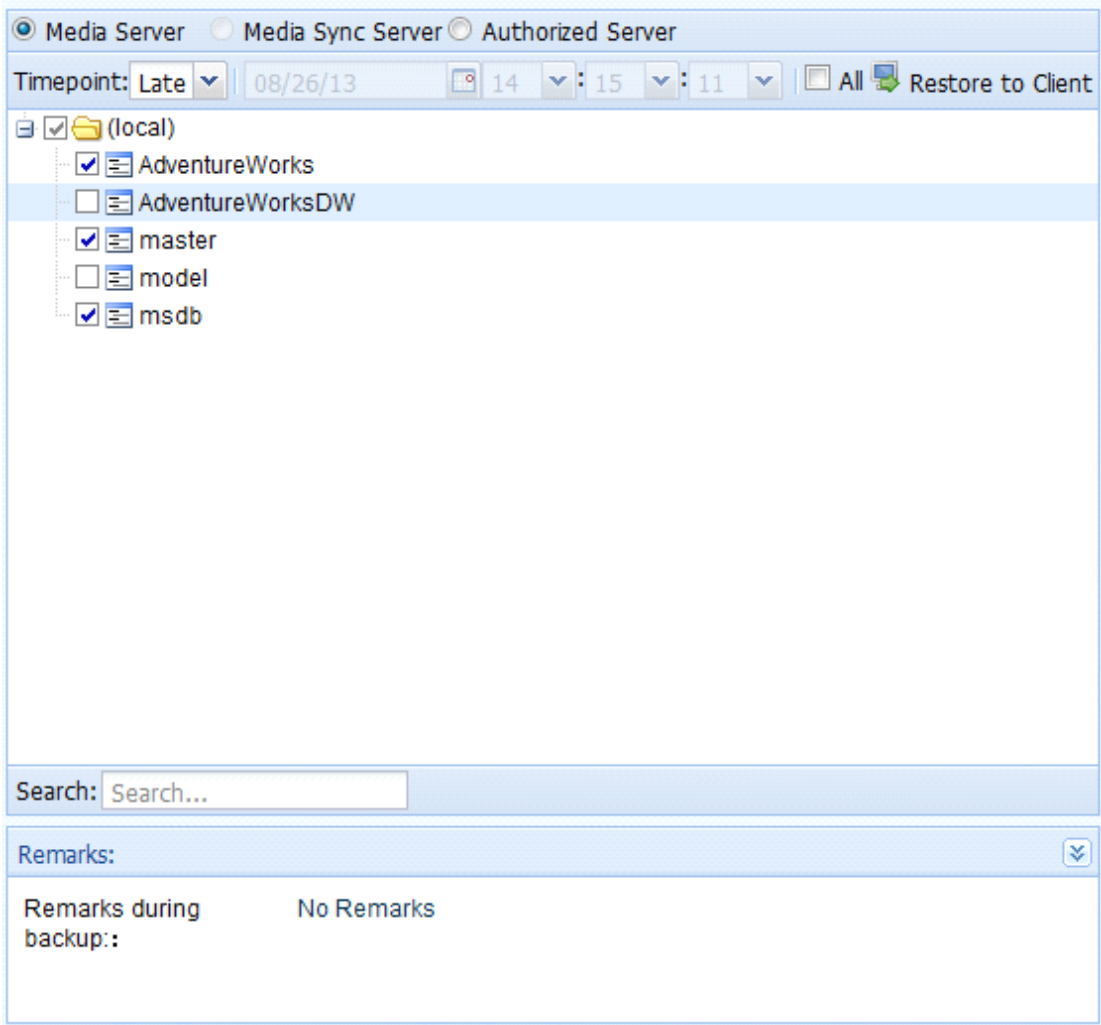

Figure 74 Browse data source

Step 4: Click [Restore to Client] and select the client to be restored to. Then enter the new database name or new storage path after restoration.
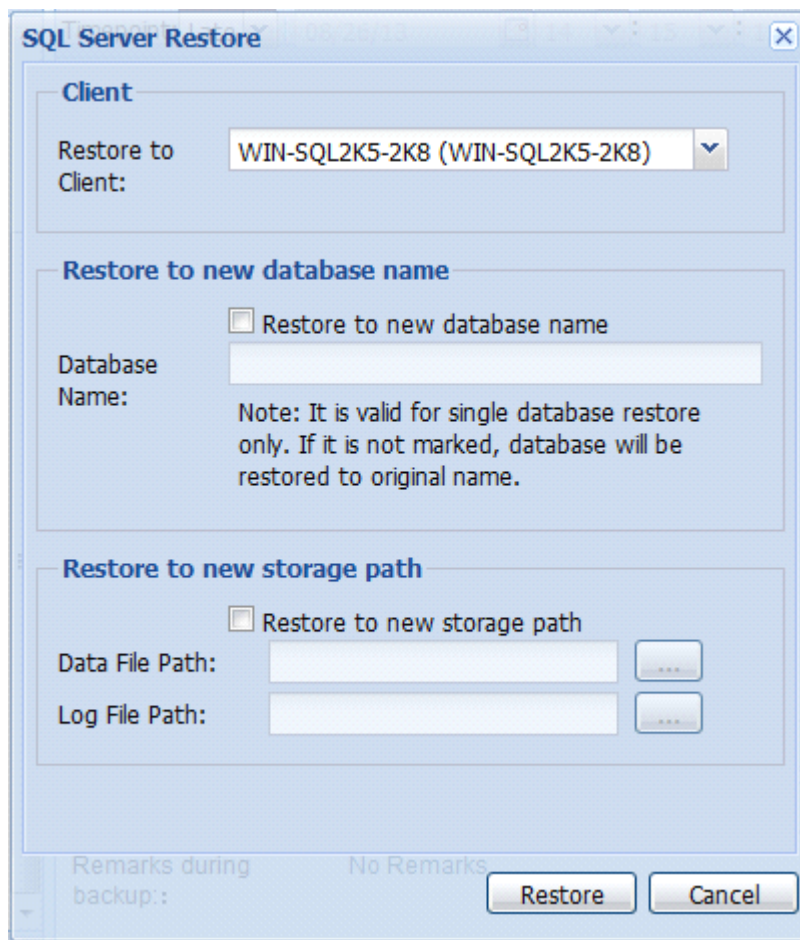
Figure 75 Restore to client

Step 5: Click [Restore] to submit the restore to execution queue.

6.4.4.2 Regular Backup and Restore for Oracle

◆ **Function Overview**

Oracle is a large relational database based on Structured Query Language (SQL). It is one of the most popular Client/Server structure databases. Its physical structure includes data file, log file and control file.

Oracle backup can be divided into cold backup and hot backup. Hot backup can be divided into full backup, incremental backup and transaction log backup further.

Cold Backup: back up files (control file, data file, online log file) when Oracle database service stops. It always coordinates system backup to perform backup and restore for the whole business system. Critical system restore and database migration are two typical situations.

Hot Backup: back up when database is normal. Compared with cold backup, it does not need to stop database. Thus it is usually used for backups when business system cannot be stopped. An administrator will select the database to be backed up on the console and rman script will be generated and sent to client. The client

creates connection with database and executes the rman script. Then the Oracle database calls the media management library to send backup information (file name, data content, etc) to channel. Then client reads channel content and send to console. The console accepts data and stores it.

Hot backup can be divided into:

Full Backup: back up whole data file of the database, which requires a long time and occupies a large amount of space.

Incremental Backup: back up the changed data since last full backup or incremental backup. It may require less time and space.

Transaction log backup: back up the archive log of database.

◆ **Notice of Deployment**

1. Make sure there is enough space on media, otherwise backup will fail and data cannot be restored.

2. The bit of client should be consistent with that of Oracle database on server, otherwise oci library of Oracle cannot be loaded.

3. Bracket or other characters similar cannot be contained in the installation path of client, otherwise error will occur.

4. Ensure $ORACLE_HOME is the installation path of Oracle database, and ensure $ORACLE_HOME/bin is contained in $PATH, as the library file needs to be loaded.

5. Check whether you have installed the client or other products before. If yes, remove it first.

6. Ensure the network is stable, otherwise data cannot be transferred.

◆ **Notice of Backup**

1. The Oracle user should have the permission of DBA, as all data needs to be backed up, including control file.

2. Archive mode needs to be started. It is a must in hot backup for Oracle.

3. Make sure there is no exception on Oracle monitor, as the instance name of backup data source is specified. To back up specified instance, specify instance name when connecting, where monitor program is needed.

4. Make sure Oracle database is open. Hot backup is not available in non-open status.

◆ **Create Cold Backup for Oracle**

Premise

1. Perform file backup for Oracle component file for data integrity. Oracle database must be closed.

2. Cold backup for Oracle RAC is not supported.

Content

1. Parameter file of original Oracle database. To simplify operation, back up the installation directory of the whole Oracle. If database file is under this directory, back up together.

2. Component file of Oracle database (control file, data file, online log file).

Backup Procedure

Step 1: Confirm database components

➢ Locate the path of database name and component file via sqlplus tool:

➢ Locate database name: select name from v$database;

➢ Locate data file path: select name from v$datafile;

➢ Locate control file path: select name from v$controlfile;

➢ Locate path of online log file: select member from v$logfile;

Step 2: Stop server

Stop the Oracle database service after confirming the path of all these files by running command of shutdown immediate in sqlplus, or by stopping Oracle service in service management of Windows server (Please make sure this database is not used by front-end applications).

Step 3: Back up

Create a file backup job to back up the installation directory and component files of this server.

Step 4: Start database service

After full backup, start Oracle database service to ensure normal restore of original database. You can start by using the startup command in sqlplus or start by the service in service management of Windows.

◆ **Create Hot Backup for Oracle**

Configure Client

Log in to the system by using an admin account and select [System]/[Client] to switch to the client management interface. Click [Configure] to mark Oracle as database type. Then click [OK].

Create Job

Step 1: Enter [Backup] and click [New] to display the dialog box of [New Backup Job Wizard]. Select [Database Backup/Oracle] and click [Next].

Step 2: Enter job name, job group, destination and data type. Then click [Next] to continue.

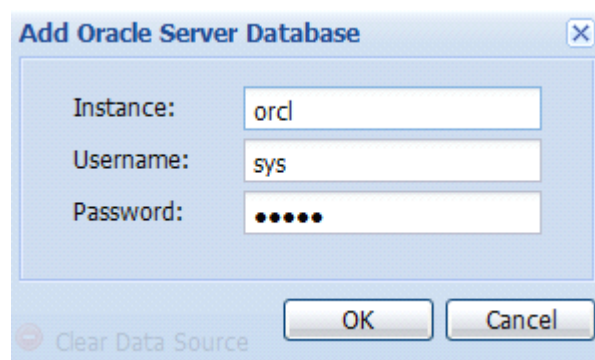Step 3: Enter [Data source] and click [Add Oracle database] to enter password.

Figure 76 Add Oracle Server Database

Unfold the client to be backed up, select Oracle database and all table space.
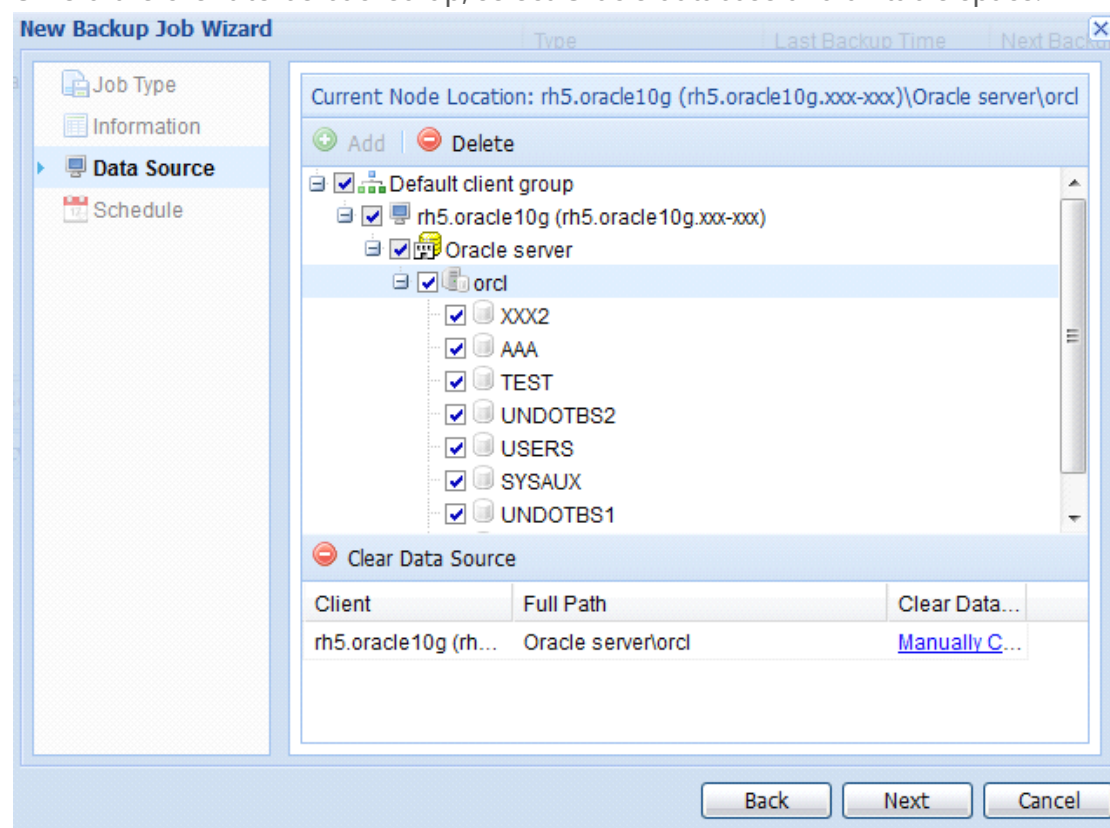

Figure 77 Select data source of Oracle Backup

Step 4 Enter [Schedule/Event] to configure detailed job schedule via "add, modify, delete". You can also configure media option, compression/encryption and flow control in [Options]. Click [OK] to finish creation.
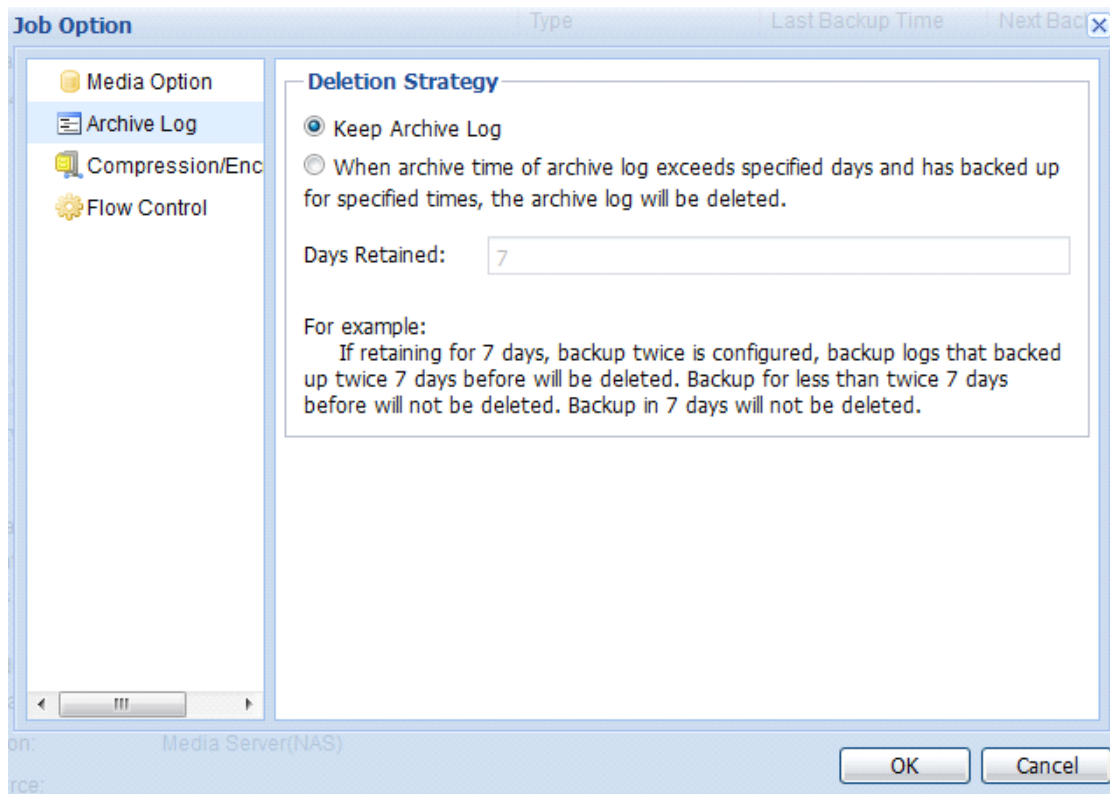
Figure 78 Configure archive log of Oracle

➢ Archive log needs to be configured for transaction log backup only. The backup logs over retention day will be deleted.
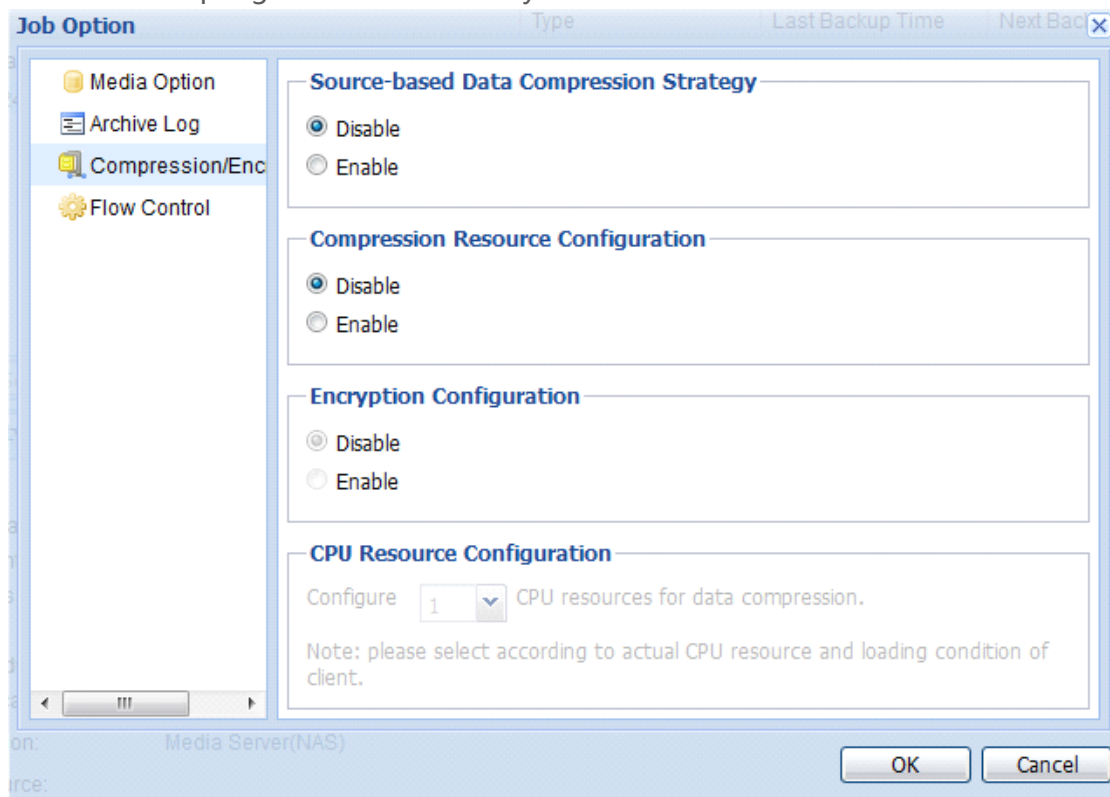

Figure 79 Configure data compression of Oracle

➢ Data compression supports transferring data to media server after compression, and saving in OFS system file to enhance backup speed and

reduce the space required. Furthermore, data encryption is supported to ensure data security.

➢ The default compression and encryption configuration is "Disabled". When compression/encryption is enabled, CPU resource count, which is defaulted by 1, can be configured between 1 and 6 according to own needs. If it exceeds the actual CPU resource count available, it will adjust automatically.

➢ Advanced compression compresses source-based data. It compresses when backing up data file via rman, but not to other files. Oracle 10g and Oracle 11g are supported.

➢ Standard compression compresses data by selecting appropriate CPU count based on actual CPU resource and loading condition. All versions are supported.

➢ Either or both compression methods can be selected.

◆ **Configuration of Best Backup Strategy**

For better protection for your Oracle server, we provide a best backup strategy. But it is recommended that you configure based on your situation.

1. For production database, we recommend performing one full backup every week and one incremental backup every day. Full backup can be done at weekends and incremental backup can be done during evenings.

2. If there is not much data, or space is sufficient, we recommend doing two full backups every week, depending on user environment.

3. Data of one month can be retained, that is, 4 full backup copies. If more data is to be retained, you can synchronize the former backup sets to secondary media.

4. Run dbcc to check the consistency of database before backup, so as to ensure the accuracy of backup.

Example a backup strategy for reference:

➢ Sunday: full backup, transaction log backup, cold backup.
➢ Monday: level 1 incremental backup, both in the morning and evening.
➢ Tuesday: level 1 incremental backup, both in the morning and evening.
➢ Wednesday: level 1 incremental backup, both in the morning and evening.
➢ Thursday: level 1 incremental backup, both in the morning and evening.
➢ Friday: level 1 incremental backup, both in the morning and evening.
➢ Saturday: level 1 incremental backup, both in the morning and evening.

Here is the strategy for various special situations for reference:

1. The database application is rather frequent, at most 10-30 min data loss can be tolerated.

As the database application is rather frequent, we recommend performing one full backup and cold backup every two days or every day, one incremental backup every half hour, and one or multiple transaction log backups every week.

2. The database is very large

As the database is large, large storage space will be occupied by a full backup so frequent full backup is not a good decision. We recommend performing one full backup and cold backup every week, one or multiple incremental backups every day, and one or multiple transaction log backups every week.

3. The database is rather important

As the database file is rather important, and database needs to be restored to certain timepoint frequently. We recommend performing one full backup and cold backup every week, two or more incremental backups every day, transaction log backup every two days or every day, and to retain multiple transaction log copies in strategy configuration.

◆ **Note for Restore Deployment**

1. Ensure there is enough space on the client to be restored, otherwise restore will fail.

2. Ensure the network is stable, otherwise restore will fail.

◆ **Note for Restore**

1. Ensure the Oracle monitor is normal, as we need to restore to specified instance. Oracle must be connected via service.

2. For hetero-machine restore, install Oracle database program and create a database with the same name in the target machine. Which instance is backed up, which instance needs to be connected during restore.

3. For hetero-machine restore, make sure the installation path of Oracle is consistent with that of client, as there is no re-direction in restore.

4. For hetero-machine restore, check the version of Oracle, otherwise restore will fail, or the database restored cannot be used normally.

5. For hetero-machine restore, make sure the storage path of Oracle data file is in target machine. For example, if one data file of original client is stored in tablespaces of G:, this path must be exist in the target machine. Otherwise, data

write will fail, and restore will fail.

6. Make sure the Oracle database on the client can be closed by using the shutdown immediate command to ensure the Oracle database is normal. This command will be used in restore. If it cannot be stopped, it will time out and restore will fail.

7. If restoring cold backup to new server, make sure the Oracle database service of the new server is stopped.

◆ **Restore Cold Backup**

Select the backup set of cold backup and browse to restore to original location. Then start Oracle database service after restore. This is a file backup strategy. For detailed information, please refer to Best Practice for File Backup and Restore.

◆ **Restore Hot Backup**

1. Restore to Original Client

The first situation is to restore to the last consistent state. After database restore, the database will try to redo the archive log file after this backup, and restore to the consistent state before an error occurred.

Select the backup set and click [Restore to Client]. Select the original client and restore to the last consistency status. Then click [Restore].
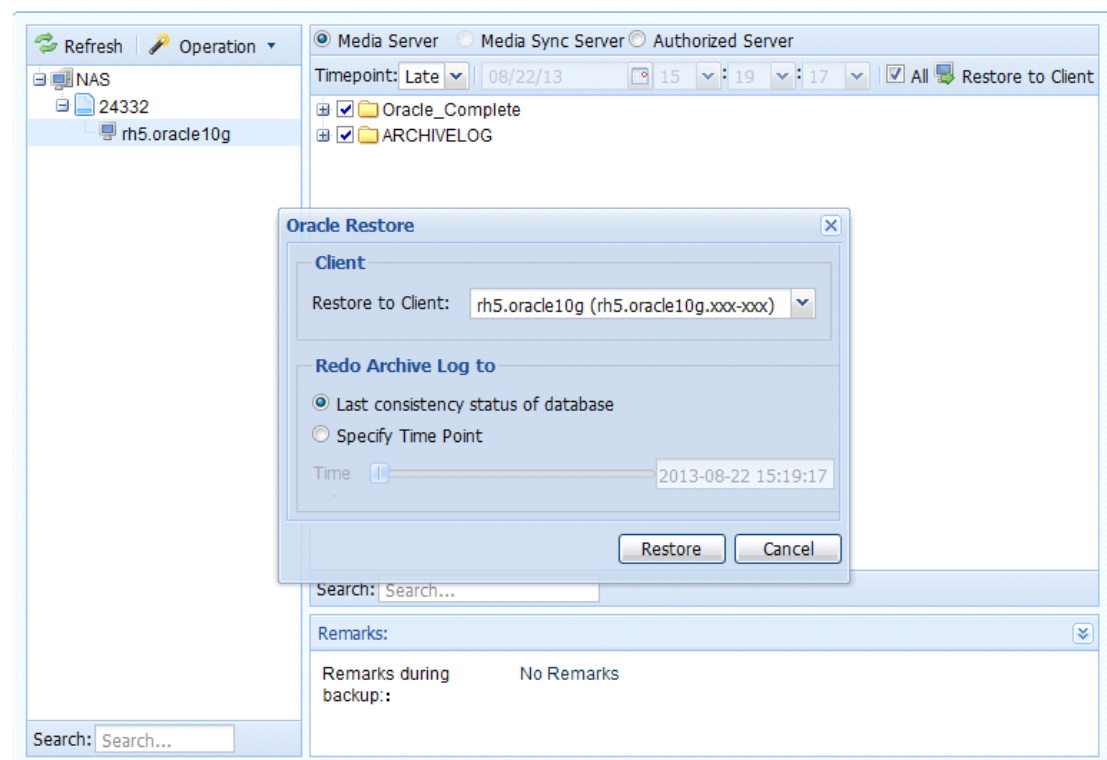

Figure 80 Restore to the last consistency status

The second situation is to redo log to specified timepoint. After database restore,

database will roll forward or redo the archive log file after this backup via the timepoint selected, and restore to the status of certain timepoint.

2. Restore to Different Machine

Step 1, delete all data files on target database

Delete all Oracle data files on target server (that is, control file, log file, and data file).

The procedure is to locate the path of the data file, control file and online log in sqlplus and close the database. Then delete related file in the system.

Step 2, restore data file and control file

Select the client to be restored to restore to the last consistent state. Then click [Restore].

6.4.4.3 Regular Backup and Restore for Active Directory

◆ **Function Overview**

Active Directory is directory service for Windows Standard Server, Windows Enterprise Server and Windows Datacenter Server. It stores relative network information by structured data. AnyBackup Appliance supports Active Directory backup and restore on Windows Server 2003 and later versions.

◆ **Backup Wizard**

Configure Client

Log in to the system via admin account and select [System]/[Client] to switch to the client management interface. Click [Configure] to mark Active Directory as database type. Then click [OK].

Create Job

Step 1: Enter [Backup] and click [New] to display the dialog box of [New Backup Job Wizard]. Select [Database Backup/Active Directory] and click [Next].

Step 2: Enter job name, job group, destination and then click [Next] to continue.

Step 3: Enter [Data Source] to select target client. Unfold instance node and select the database to be backed up. Click [Next].
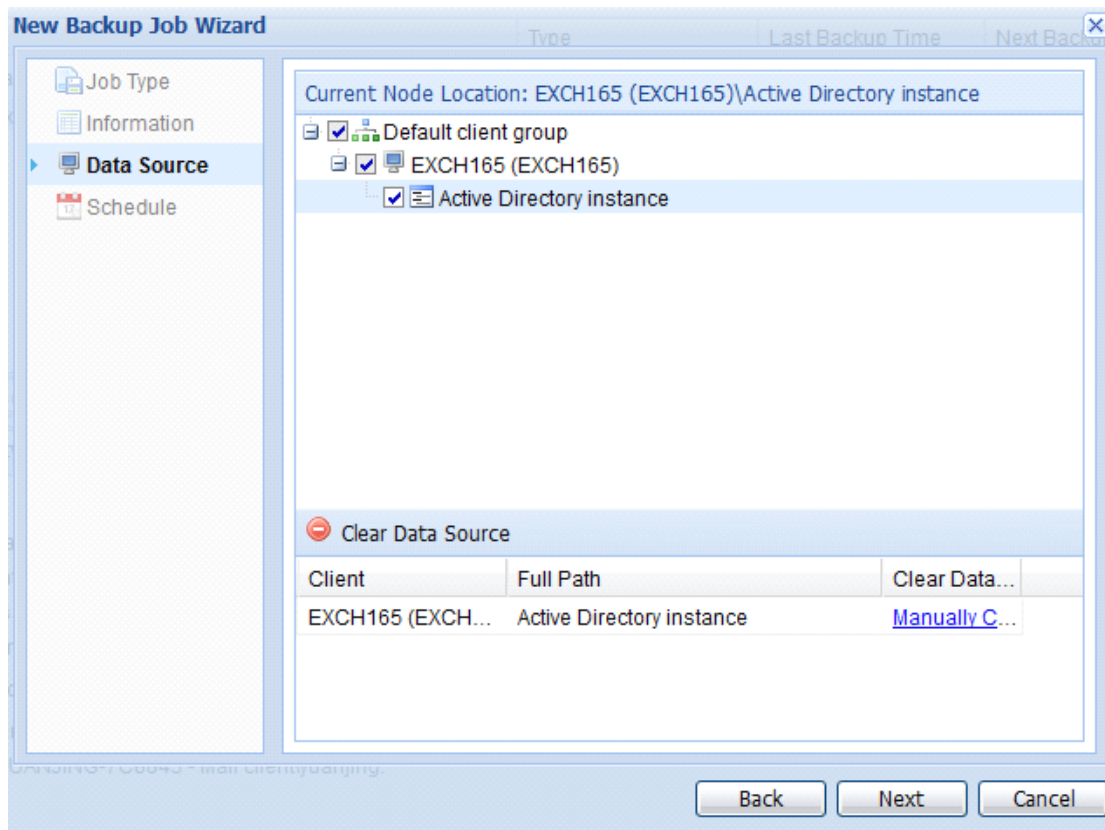
Figure 81 Select data source

Step 4: Configure schedule and event in [Schedule/Event] and then click [Done]. Click [Backup] to submit the Active Directory backup job.

◆ **Restore Wizard**

Notice for Restore

1. Directory Restore Mode

When performing AD restore, AD domain controller needs to enter the directory restore mode, otherwise the restore will fail.

2. Hetero-machine Restore

AnyBackup Appliance does not support to restore AD to another AD domain controller directly, nor to restore to the AD domain controller rebuilt directly. It will cause domain controller not available, or even blue screen, please be cautious.

If you want to achieve hetero-machine restore for AD, please perform hetero-machine restore for system first, and then to AD database.

Restore Operation

Step 1: Restart AD domain controller and press F8 to enter advanced mode. Select "Directory Service Restore Mode".

Step 2: Log in to the Management Console and click "Backup and Restore/Restore/" to switch to the browse to restore page.

Step 3: Unfold media server/media sync server, unfold the job list to select the AD backup job to be restored and select the client for restore.
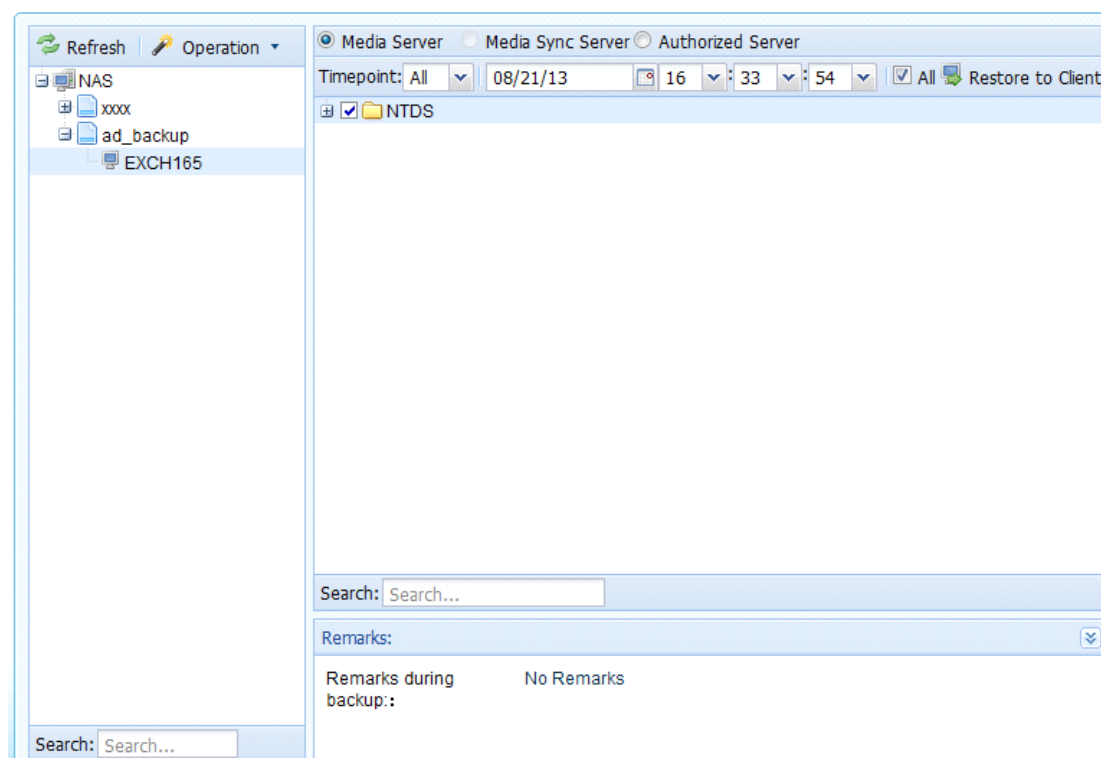

Figure 82 Select the client to be restored

Step 4: Click [Time Point] and select one time point to be restored.

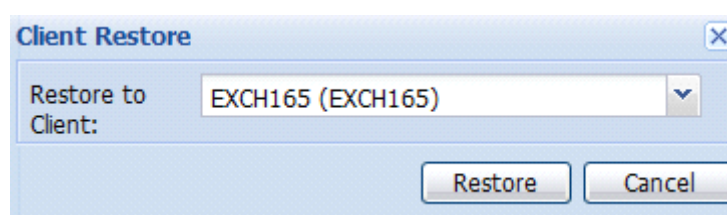Step 5: Select the whole NTDS folder in data source and click [Restore to Client].

Figure 83 Restore to client

Step 6: Click [Restore] to display the risk warning, click [OK] to submit to the execution queue.

6.4.4.4 Regular Backup and Restore for Sybase

◆ **Function Overview**

Sybase is typical large-scale database system under client/server environment of UNIX or Windows NT. AnyBackup Appliance supports backup and restore for Sybase 12.5 or later.

◆ **Backup Wizard**

Configure Client

Log in to the system by using the admin account and select [System]/[Client] to switch to the client management interface. Click [Configure] to mark Sybase as database type. Then click [OK].

Create Job

Step 1: Enter [Backup] and click [New] to show the [New Backup Job Wizard] dialog. Select [Database Backup/Sybase] and click [Next].

Step 2: Enter job name, job group, destination and decide whether to configure data deduplication. Then click [Next] to continue.

Step 3: Enter [Data Source] to add instance. Select the database to be backed up and click [Next].
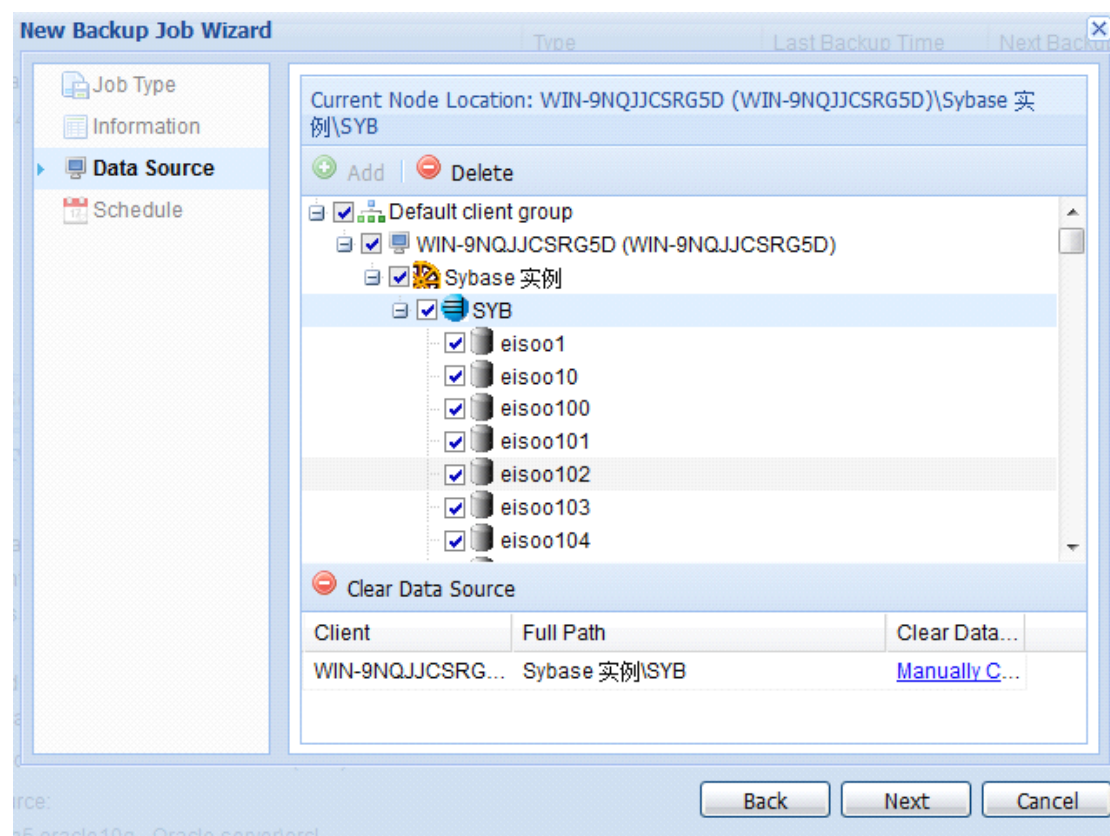
Figure 84 Select Data Source

Step 4 Enter [Schedule/Event] to configure detailed job schedule via "add, modify, delete". You can also configure media option, compression/encryption and flow control in [Options]. Click [OK] to finish creation.

◆ **Restore Wizard**

Notice for Restore

➢ Support restoring Sybase database to another machine. When performing hetero-machine restore, please ensure the database version, bit,

installation path and instance on the target machine are same, and there is a device file and database of the same name and same size.

➢ Support restoration of single database. If multiple databases are backed up in one job, you can select one or multiple database to restore. If there is a relationship among databases, they should be restored simultaneously.

➢ If you want to restore a single database to another client, create a database of the same size as the original one before restore.

➢ When restoring a database, the database will be locked. If it is being used, the lock will fail.

➢ When restoring master database, the Sybase service will be restarted via single user mode. After restoring, this service will be started via multi-user mode. Stop all applications linked with Sybase before restoring to avoid data loss.

Restore Operation

Step 1: Log in to the Management Console and click "Backup and Restore/Restore/" to switch to the browse to restore page.

Step 2: Unfold media server/media sync server, unfold job list to select the job to be restored. Then select the client for restore.
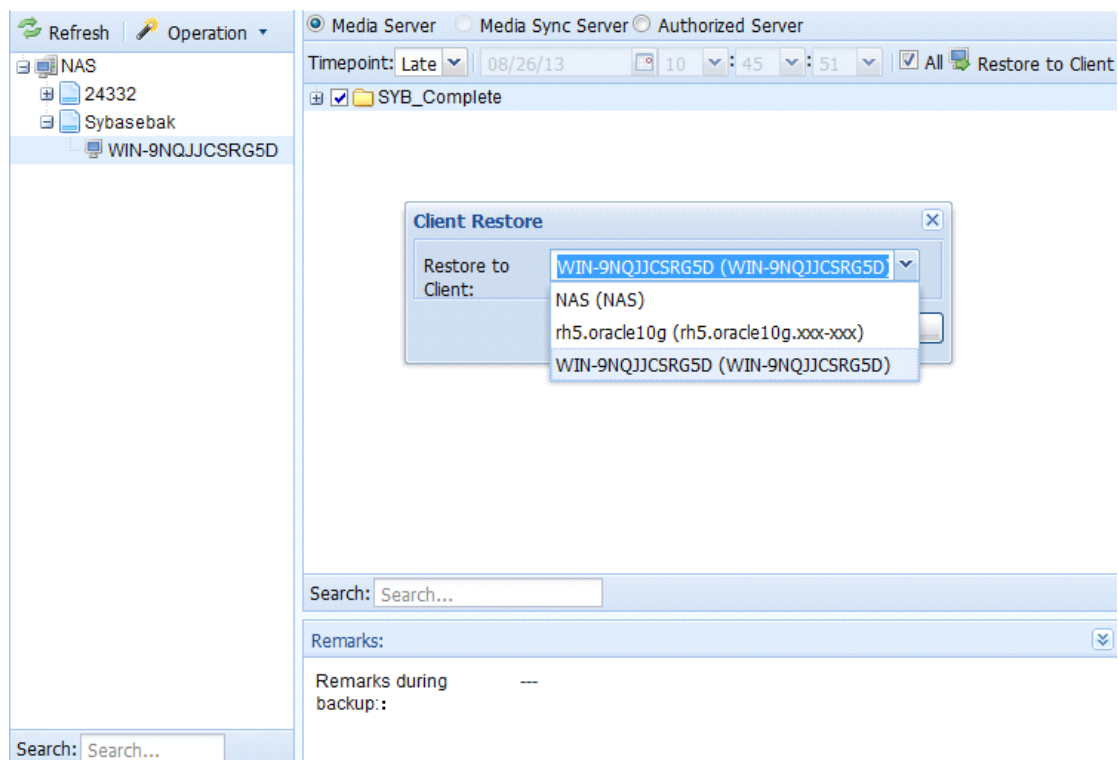

Figure 85 Restore to Client

Step 3: Click [Time Point] and select one time point. Then select the Sybase database to be restored.

Step 4: Click [Restore] to display the risk warning, then click [OK] to submit to the execution queue.

6.4.4.5 Regular Backup and Restore for Lotus Domino

◆ **Function Overview**

Domino is the market leader in collaboration platforms. AnyBackup Appliance supports full and incremental backup for Lotus Domino in Windows and Linux, and supports restoration to the timepoint of full/incremental backup or to another client.

◆ **Backup Wizard**

Note: if client is installed on Liunx, please add ltsserver.config file in AnyBackupClient and add full path of the notes.ini file in the Domino server and each Domino service line to ltsserver.config file.

E.g: /local/notesdata/notes.ini.

Configure Client

Log in to the system by using an admin account and select [System]/[Client] to switch to the client management interface. Click [Configure] to mark Lotus Domino as the database type. Then click [OK].

Create Job

Step 1: Enter [Backup] and click [New] to show the dialog box of [New Backup Job Wizard]. Select [Database Backup/Domino] and click [Next].

Step 2: Enter job name, job group, destination and configure whether to perform data deduplication. Then click [Next] to continue.

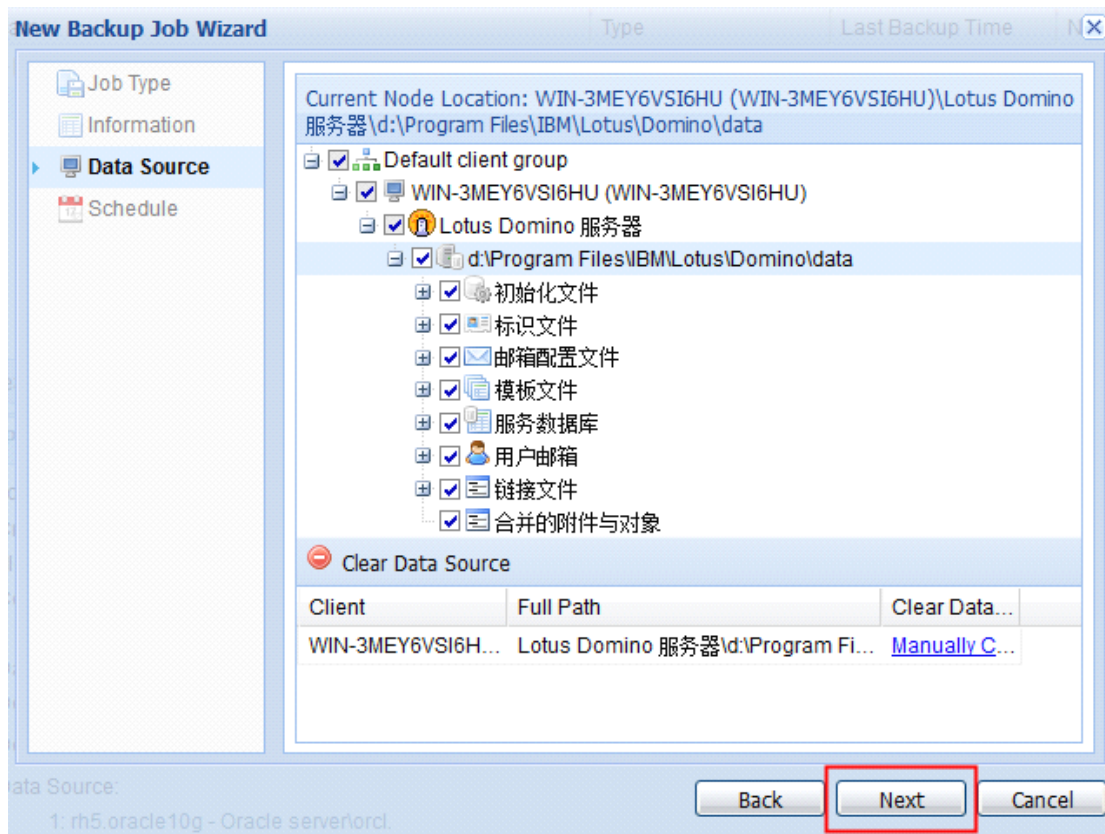Step 3: Enter [Data Source] to unfold the client to be backed up, and then unfold Lotus Domino database.

Figure 86 Select Data Source

Step 4: Enter [Schedule/Event] to configure detailed job schedule via "add, modify, delete". When configuring [Start Time], try to select the time when server is free. When configuring [Retention Strategy], take storage space and data demand into consideration. Then click [Done] to exit the backup job wizard.

Step 5: You can also configure media options, compression/encryption and flow control in [Options]. Click [OK] to finish creation.

◆ **Restore Wizard**

Step 1: Close Domino service.

Step 2: Log in to the system and click "Backup and Restore/Restore/".

Step 3: Unfold media server/media sync server, unfold job list to select the Domino backup job to be restored, and then select the client.
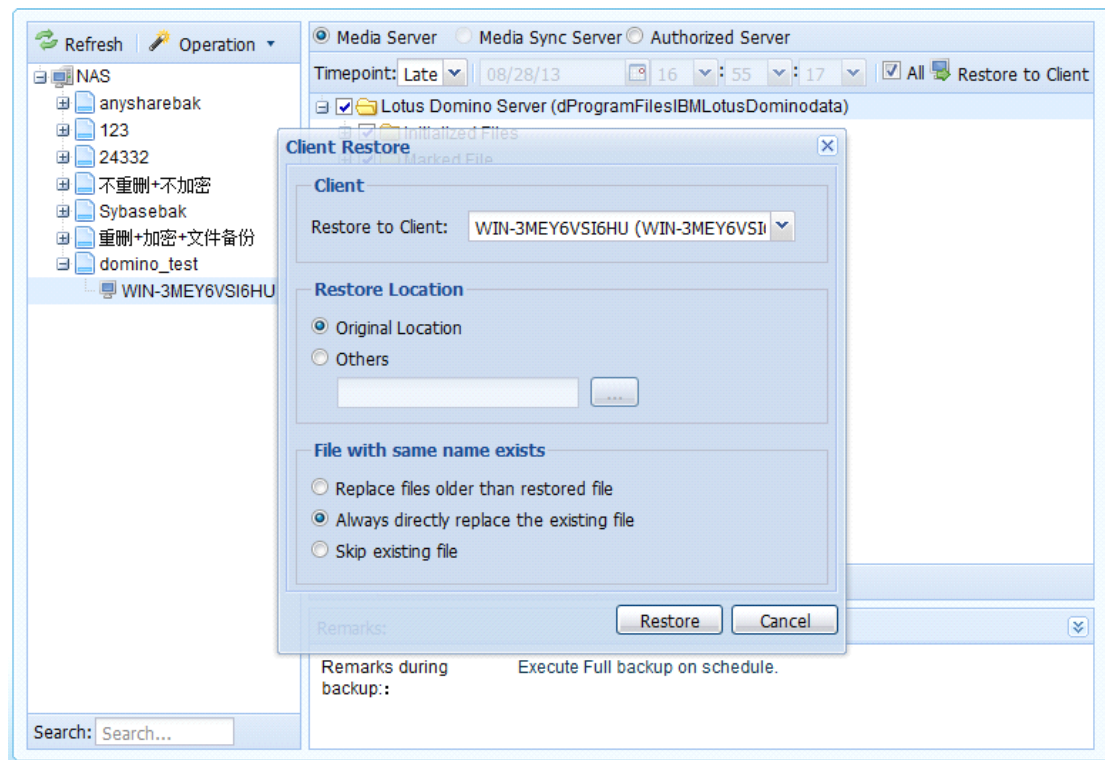
Figure 87 Select the client　to be restored

Step 4: Click [Time Point] and select one time point.

Step 5: Select the database to be restored in data source and click [Restore to Client].

Step 6: Click [Restore] to show the risk warning. Click [OK] to submit to the execution queue.

6.4.4.6 Regular Backup and Restore for Exchange Server

When making online continuous backups for Exchange Server via EDK port, users do not need to stop Exchange Server database services, nor do they need to switch the database status. The backup execution will not pose evident impact on the performance of Exchange Server. Usually, when making a full backup for Exchange Server, all the database files and log files will be backed up. After the backup, a truncation operation will be done to transaction log files. The transaction log files which have been backed up will be deleted, and then the backup time point will be recorded. Additionally, when making incremental backups for Exchange Server, all the database log files will be backed up. After the backup, a truncation operation will also be done to transaction log files.

Two kinds of backup are supported, namely full backup and incremental backup.

(1) Full Backup

Back up the selected data information of database; including database file, log file and checkpoint file. Compared to incremental backup, full backup requires more storage space and time so it should be performed less often than incremental backup.

(2) Incremental Backup

Back up the changes since last full backup. It backs up transaction log files only, not the current database. The full backup is the basis for incremental backup. When restoring, restore the full backup first and then the incremental backups. Compared with full backup, incremental backup takes longer to restore.

◆ **Backup Wizard**

Configure Client

Log in to the system by using the admin account and select [System]/[Client] to switch to the client management interface. Click [Configure] to mark Exchange Server as database type. Then click [OK].

New Job

Step 1: Enter [Backup] and click [New] to show the [New Backup Job Wizard] dialog. Select [Database Backup/Exchange Server] and click [Next].

Step 2: Enter job name, job group, destination and data type. Then click [Next] to continue.

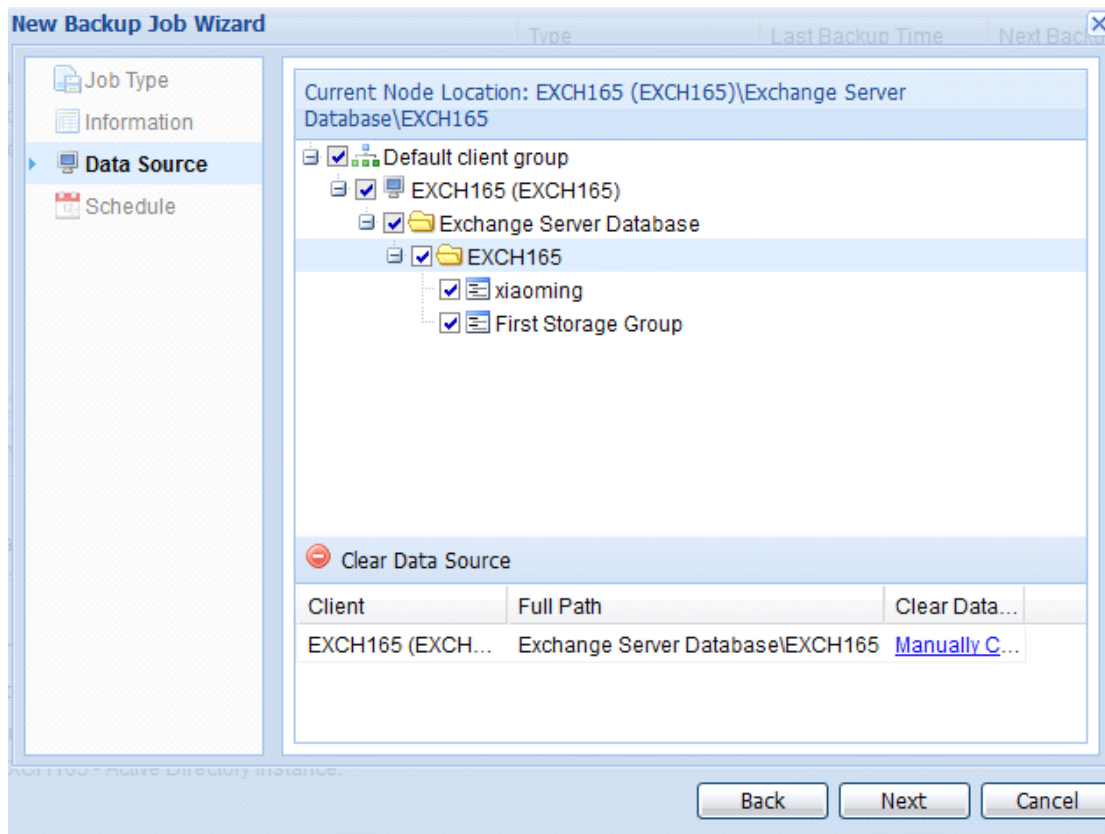Step 3: Enter [Data Source] to unfold the client to be backed up, and then unfold Exchange Server database.

Figure 88 Select Data Source

Step 4 Enter [Schedule/Event] to configure detailed job schedule via "add, modify, delete". You can also configure media option, compression/encryption and flow control in [Options]. Click [OK] to finish creation.
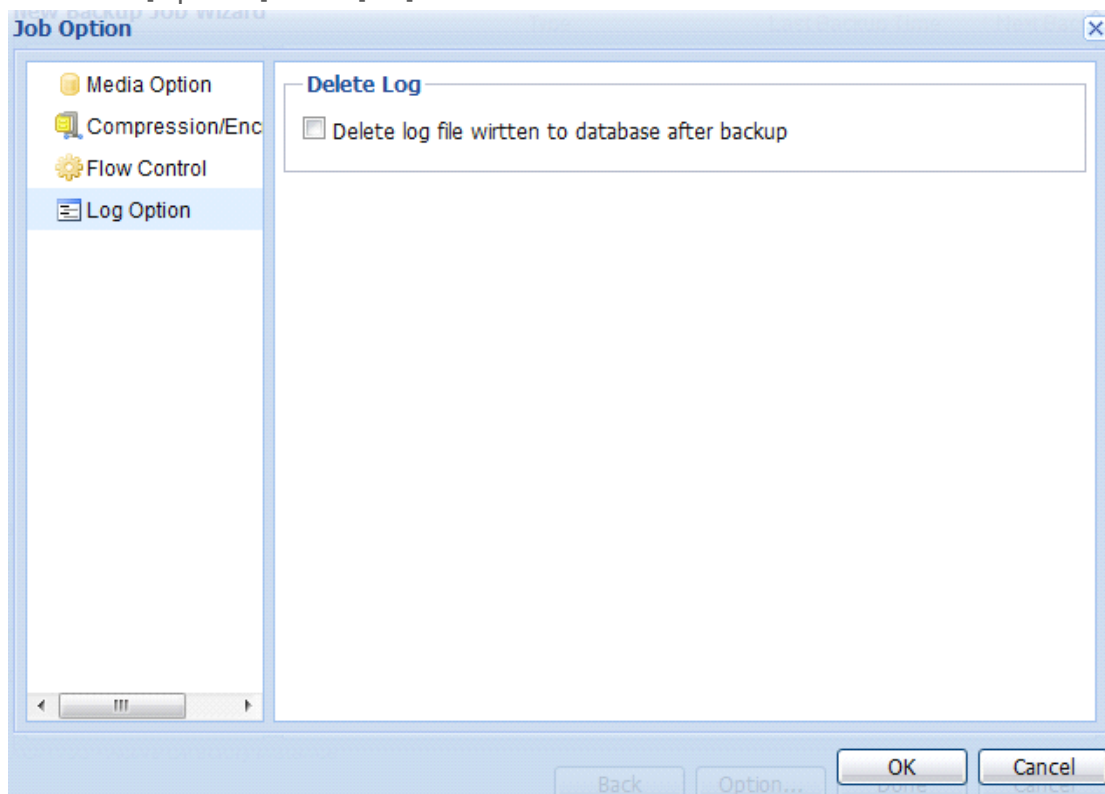

Figure 89 Log Option

> ➢ Log options support deletion of log file written into database file after backup.

🔔 **Note:** We recommend creating one job for each client, and select the whole server to back up.

◆ **Best Backup Strategy**

- ➢ Job Schedule: full backup every weekend+incremental backup every day (adjust as required).
- ➢ Try to configure the start time when server is free.
- ➢ Retain data for one month (4 full copies), depending on storage space and storage time.

◆ **Restore Wizard**

Notice for Restore

1. Hetero-machine Restore (Non Exchange DAG)

AnyBackup Appliance does not support restoring to other servers with Exchange Server installed, otherwise errors will be caused.

2. Exchange DAG Restore

If the server with the active copy is changed during backup or before, restore the database to the server of its active copy.

If restoring database to the server of passive copy, it will not restore by default.

3. Storage Path of Database File and Log File

The storage path of database file and log file for restore must be consistent with that of backup, otherwise errors will be caused.

Restore Operation

Step 1: Log in to the Management Console and click "Backup and Restore/Restore/" to switch to the browse to restore page.

Step 2: Unfold media server/media sync server, and select the SQL Server job to be restored in job list. Then select the client for restore.
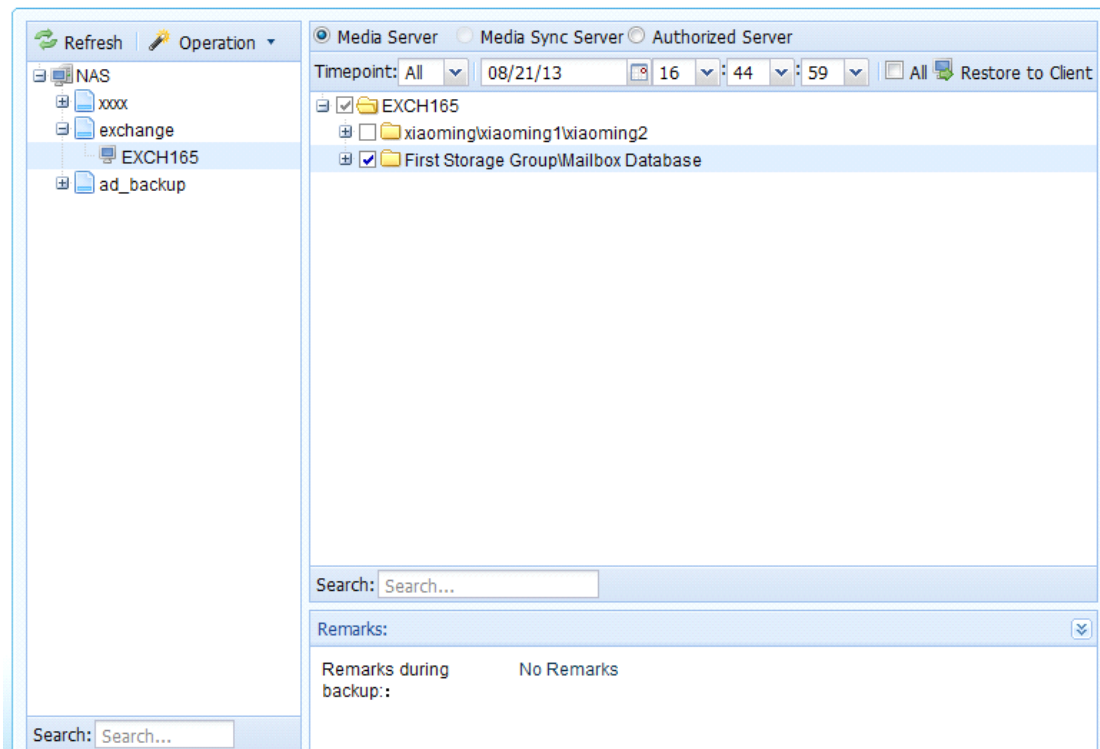
Figure 90 Select data source to be restored

Step 3: Click [Time Point] and select one time point. Unfold data source to select the database to be restored and click [Restore to Client].
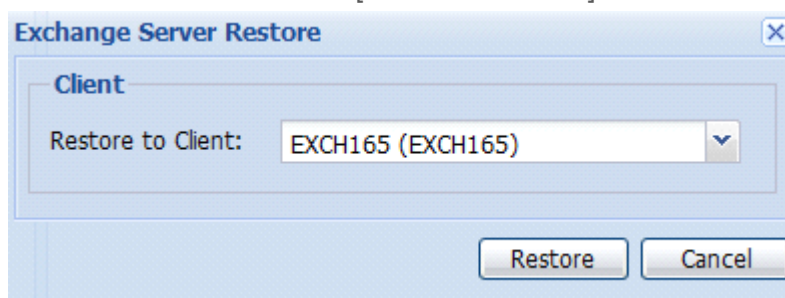

Figure 91 Restore to client

Step 4: Click [Restore] to show the risk warning and click [OK] to submit to execution queue.

ℹ️ **Note:** After restore, the database status will be Uninstall. Install it manually before using it.

6.4.4.7 Regular Backup and Restore for DB2

◆ **Function Overview**

DB2 database supports offline and online backup itself. AnyBackup Appliance is C/S structure and uses online backup for DB2, which is composed of full backup, incremental backup and differential backup.

Full Backup: back up the selected data source to specified backup set. This backs up all data to OFS media and generates a timepoint to record the backup contents.

Incremental Backup: based on last full backup and back up data source to OFS media. It backs up changed and increased file only, thus avoiding repeat backup for the same files. If full backup has never been done, incremental backup will change to full backup automatically.

Differential Backup: based on last full or incremental backup. It backs up new data to OFS media and generates a timepoint.

◆ **Notice for Backup**

1. Modify rotation log mode to archive log mode

(1) Create a directory on the disk which has enough space to store archive log file. The destination of archive log should be separate from that of active log file. We recommend creating a new folder to store the archive file.

(2) Interrupt the connection with database using a command like: TERMINATE.

(3) Update the destination of archive log file (Specify the path of archive log file has the same effect with open archive log mode), such as: db2 update db cfg for db_name using logarchmeth1 "Disk:e:\db_name\archive".

1) Here, if you want to reconnect to database, such as: db2 connect to db_name, an error of "SQL1116N A connection to or activation of database db_name cannot be made because of backup pending: SQLSTATE=57019" will occur. As a full database backup is needed to change log mode from rotation to archive, even if full backup has been done in rotation log mode.

2) Perform a full database backup via command line, such as: BACKUP DATABASE db_name TO d:\db_name\backup.

3) Try to reconnect to the database and it will succeed, using a command like CONNECT TO db_name.

2. Configure incremental backup for database

Incremental backup will not be available until trackmod mode is configured on. The configuration way is:

1) Connect database: connect to database.

2) Check the trackmod parameter in database configuration: db2 get db cfg for database | find /I "trackmod". If using Linux, use db2 "get db cfg for database" | grep TRACKMOD.

3) If trackmod is off, use the command to open it: db2 update db cfg for database using trackmod "on". But it will take effect in next activity.

3. Does not support backup for single table.

4. The instance name, username and password of backup and restore end must be consistent.

5. Database service must be enabled when creating and executing backup job, otherwise data source cannot be added.

◆ **Backup Wizard**

Check and Configure DB2 Environment

Step 1: Make sure bin directory of DB2 is included in system environment variable.

➤ Right click "My Computer" and select properties. Select "Advanced" and click "Environment Variable" to check whether bin directory under DB2 installation directory is contained in Path Variable.
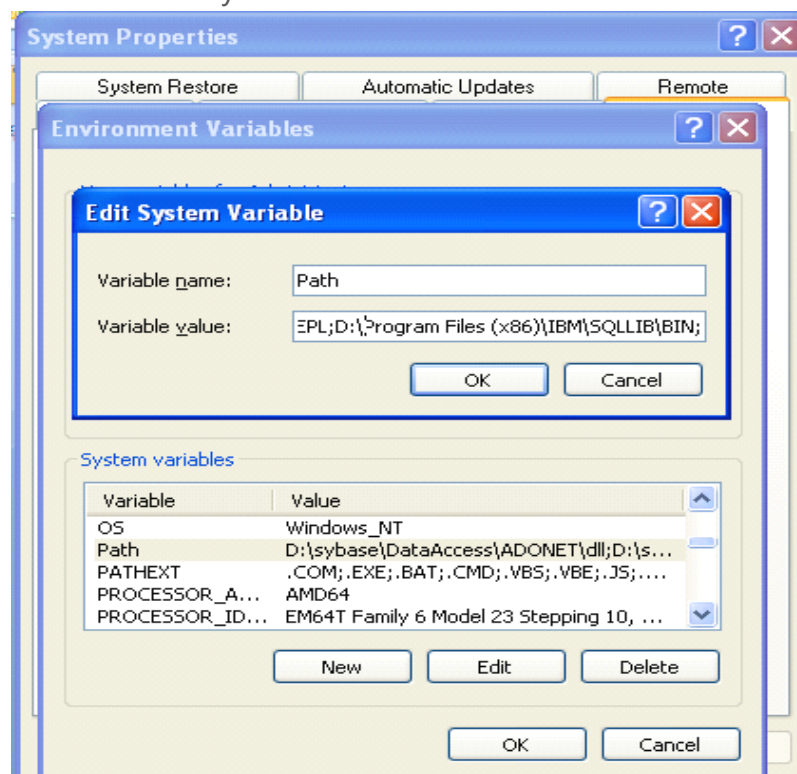
Figure 92 Configure environment variables

➤ Run "cmd" in "Start" and enter echo %path%. Search whether bin directory under DB2 installation directory is contained.
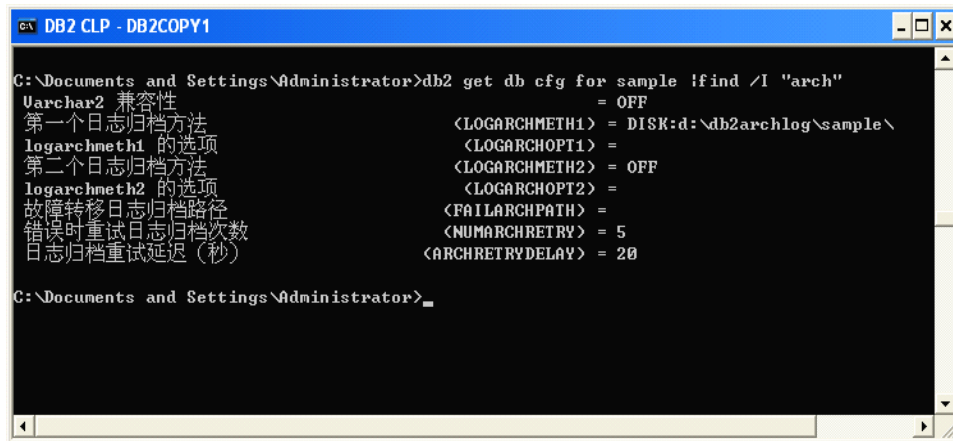
ꙮ **Note:** After DB2 is installed, bin directory is contained in system path by default.

Step 2: Check whether the database to be backed up has been configured as archive mode.

Enter db2 command window and enter:

db2 get db cfg for sample |find /I "arch",

Check whether the logarchmeth1 value is directory, here sample is database name (similarly hereinafter).
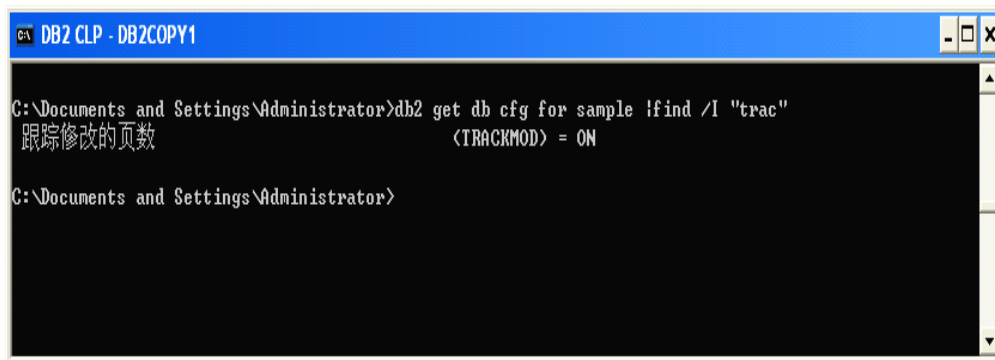
Figure 93 Check configuration

⚠ **Note:** Parameters such as logarchmeth1 are added in DB2 8.2 or later for better log management. To keep compatible with the former versions, parameters of logretain and userexit are kept. When configuring archive mode, we recommend setting logarchmeth1 on the storage media beyond data file, and mirror done is preferred.

Step 3: Check whether parameter is configured for the database for incremental backup.

Enter DB2 command window and enter: db2 get db cfg for sample |find /I "trac" to check whether the modified page is ON. Here sample is database name.

Figure 94 Check configuration

If not, please use the command: db2 update db cfg for sample using trackmod "on" to configure it ON.

Configure Client

Log in to the system by using admin account and select [System]/[Client] to switch to the client management interface. Click [Configure] to mark DB2 as database type. Then click [OK].

Create Job

Step 1: Enter [Backup] and click [New] to show the dialog box of [New Backup Job Wizard]. Select [Database Backup/DB2] and click [Next].

Step 2: Enter job name, job group, destination and configure whether to enable data deduplication. Select data selection mode and data type. Then click [Next] to continue.

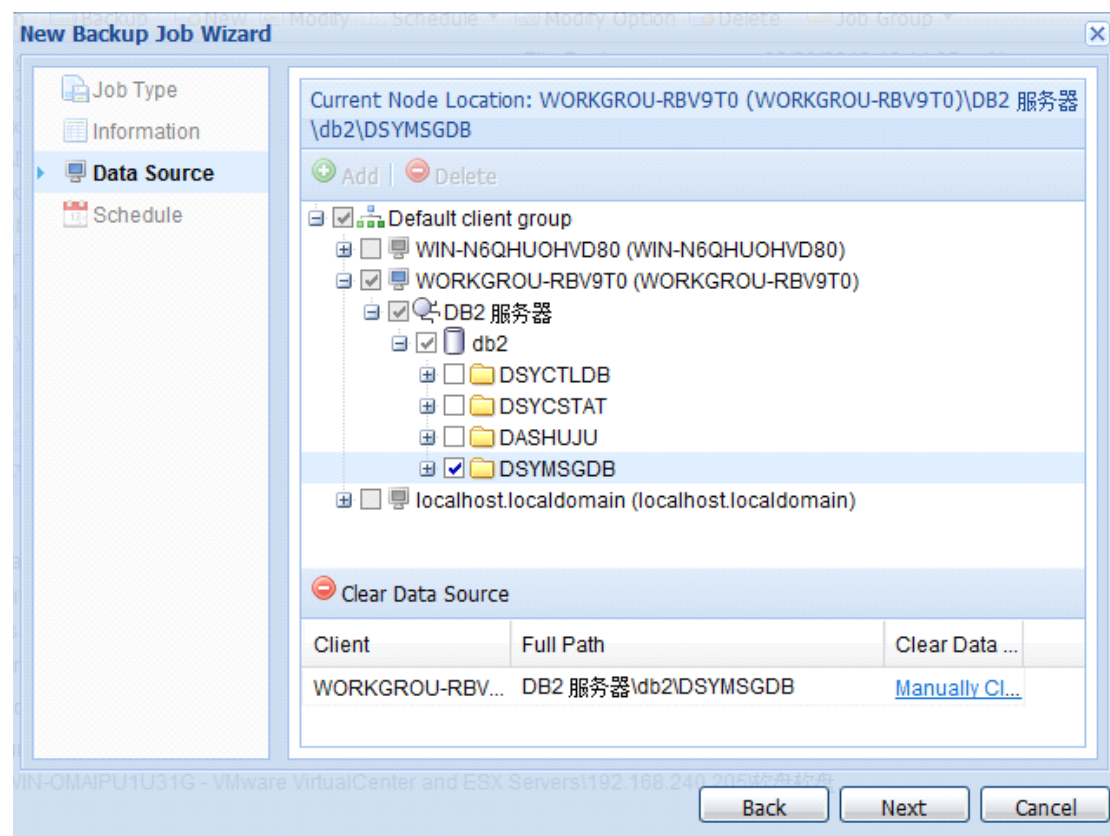Step 3: Enter "Data Source" to unfold client list to select the data source. Then click [Next] to continue.

Figure 95 Select data source

Step 4 Enter [Schedule/Event] to configure detailed job schedule via "add, modify, delete". You can also configure media options, compression/encryption and flow control in [Options]. Click [OK] to finish creation.

◆ **Configure Job Strategy**

There is no difference among full, incremental and differential backup for DB2 table space. When multiple table spaces of one database is selected as data source, data and log files of this table space will be backed up no matter what backup type is selected.

Configure strategy according to actual situation, IO demands, security demands, etc. Here we recommend a strategy for at least one-month security.

- Perform one full backup every weekend when data application is low.
- Perform one incremental backup during the evenings, every two days.
- Perform several differential backups every day, e.g. one differential backup every noon and afternoon.
- Configure to retain 4 full copies to ensure no data loss for about 28 days.
- Save log in the secure mirror area.

◆ **Restore Wizard**

Select Restore Type

Select what restore method to use according to data loss range:

- If a table is lost, you can restore table space data to specified database. A timepoint can be selected.
- If database is damaged, you can restore the whole database to the original location.
- If you want to do a replication for original database, you can restore the database and enter the name.
- It you want to restore the whole database to a former status, restore by the specified timepoint.

Select Restore Timepoint

If timepoint is specified, please make sure it is after the latest full backup. If not, an error will occur during restore.

Restore Operation

Step 1: Log in to the Management Console and click "Backup and Restore/Restore" to switch to the browse to restore page.

Step 2: Unfold media server/media sync server, unfold the backup job to be restored in the job list and select the client for restore.

Step 3: Click [Time Point] and select a time point.

Figure 96 Select the client to be restored

Step 4: Select the database to be restored and click [Restore to Client].
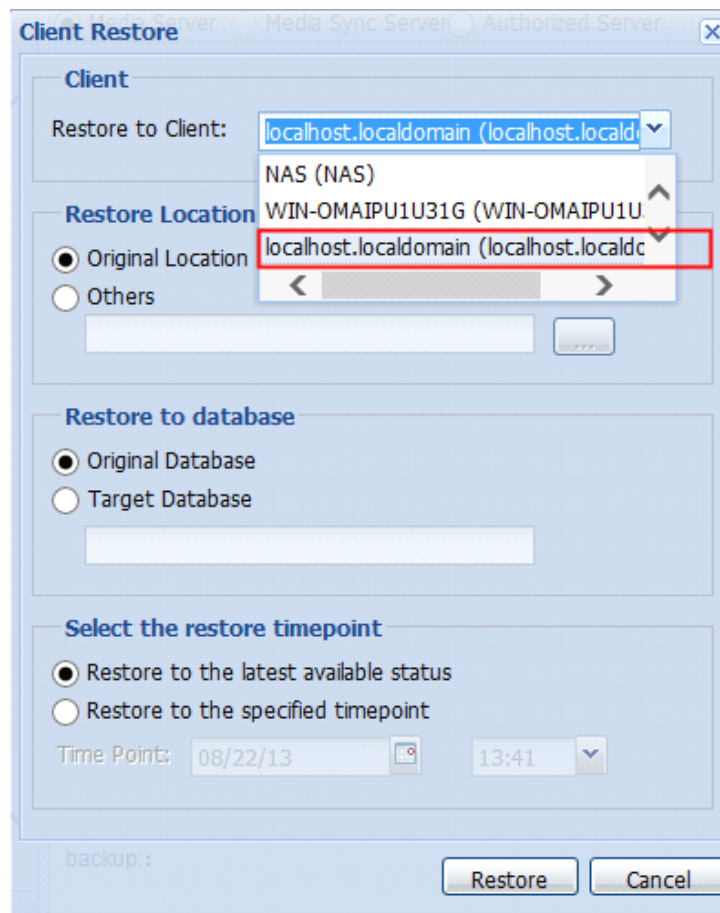
Figure 97 Restore to client

➢ Select the target machine in the drop-down menu of [Restore to Client]. If it is not selected, it will default to the original machine. If you choose to restore to another machine, make sure there is an instance of the same name.

➢ Select the original path or create a custom one in [Restore Location].

➢ If you want to restore database to a new name, check [Target Database] in [Restore to Database] and enter a new database name.

➢ In [Select Restore Timepoint], you can restore to latest state available or specified timepoint.

Step 5: Click [Restore] to displaythe risk warning and click [OK] to submit to execution queue.

6.4.4.8 Regular Backup and Restore for MySQL
◆ **Function Overview**

Script + File backup is adopted in MySQL backup. AnyBackup Appliance will first get data source and generated backup script based on the database type. Then the backup system will call backup script which can enable backup by using the built-in backup tool of the database and store backup set to temporary path. After that, the backup system will back up the backup set to the media server, and finally contents

of backup script and temporary path will be deleted.

Full backup is supported.

◆ **Notice**

1. Client Installation

a) Client version should be consistent with that of console.

b) Client contains 32-bit and 64-bit. If your MySQL version is 32-bit, you can use the 32-bit client only, even if your operating system is 64-bit. If your MySQL version is 64-bit, you can use the 64-bit client. If your client bit is inconsistent with MySQL bit, you will fail to unfold the data source.

2. MySQL Configuration

a) Before backup, MySQL database service must be running, otherwise you will fail to unfold instance.

b) Before backup, make sure MySQL environment variable is added in path, such as E:\Program Files\MySQL\MySQL Server 5.5\bin. If not, execution of backup script and restore script will fail.

◆ **Backup Wizard**
Configure Client

Log in to system by using the admin account and select [System]/[Client] to switch to the client management interface. Click [Configure] to set MySQL as database type. Then click [OK].

Create Job

Step 1: Enter [Backup] and click [New] to show the [New Backup Job Wizard] dialog. Select [Database Backup/MySQL] and click [Next].

Step 2: Enter job name, job group and select data type. Then click [Next] to continue.

Step 3: Enter [Data Source] to unfold the client to be backed up. Unfold MySQL database and click "Add MySQL Instance" to enter instance name, port, service name, username and password. Then click [Next].
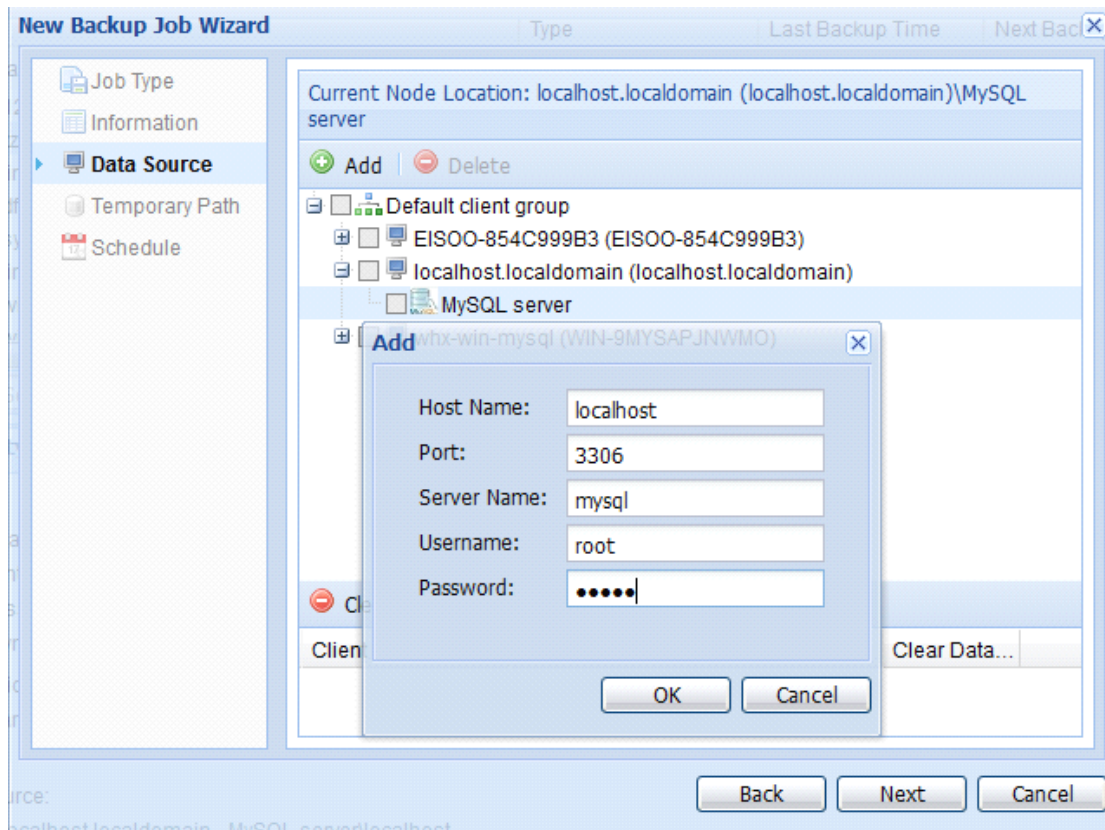
Figure 98 Add MySQL Instance

🔔 **Note:**

1. Host name refers to the host name of database. It is usually entered as localhost. It cannot be the IP address of the client.

2. Service name is not used when unfolding a data source so it will not affect backup and restore job even if service name is not entered correctly.

3. You will fail to unfold instance if the password of backend database contains special characters, such as *, as the data transfer to backend is used through the network. Special HTML characters will automatically change to usable characters. The password transferred to backend is not the real password. Modify the database password manually and add instance again.

4. Following characters are acceptable in a password ~, @, #, ￥, %、(、) ，！

5. Blank-password backup and restore is supported.

Step 4: You can see all databases under this instance by unfolding the instance. We recommend backing up all databases by selecting the whole instance.
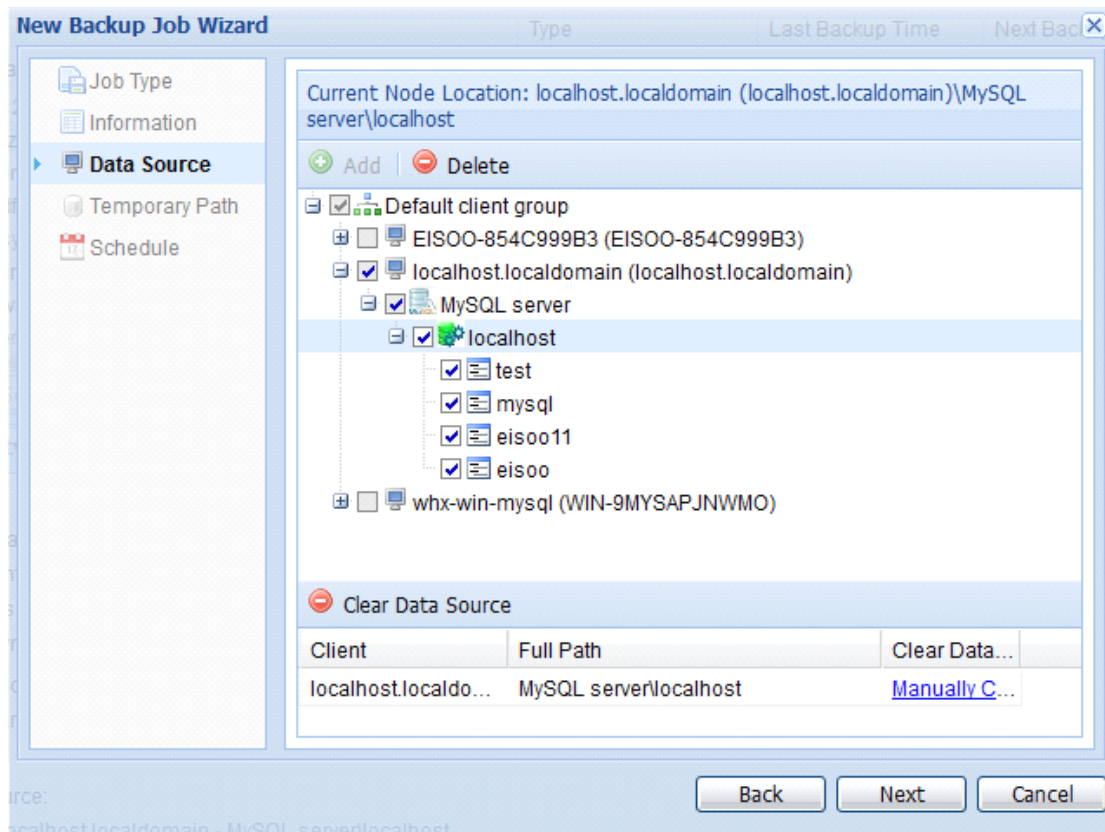
Figure 99 Select data source

🔔 Note:

1. Support backing up single database or whole instance.

2. We highly recommend not using one database in multiple jobs, as it may cause some exceptions.

3. For MySQL 5.5, system test databases, mysql and other customized databases can be viewed when data source is unfolded, but not information_schema and performance_schema.

Step 5: Enter [Temporary Path] and you can browse the temporary backup path automatically, such as E:\, click [Next].
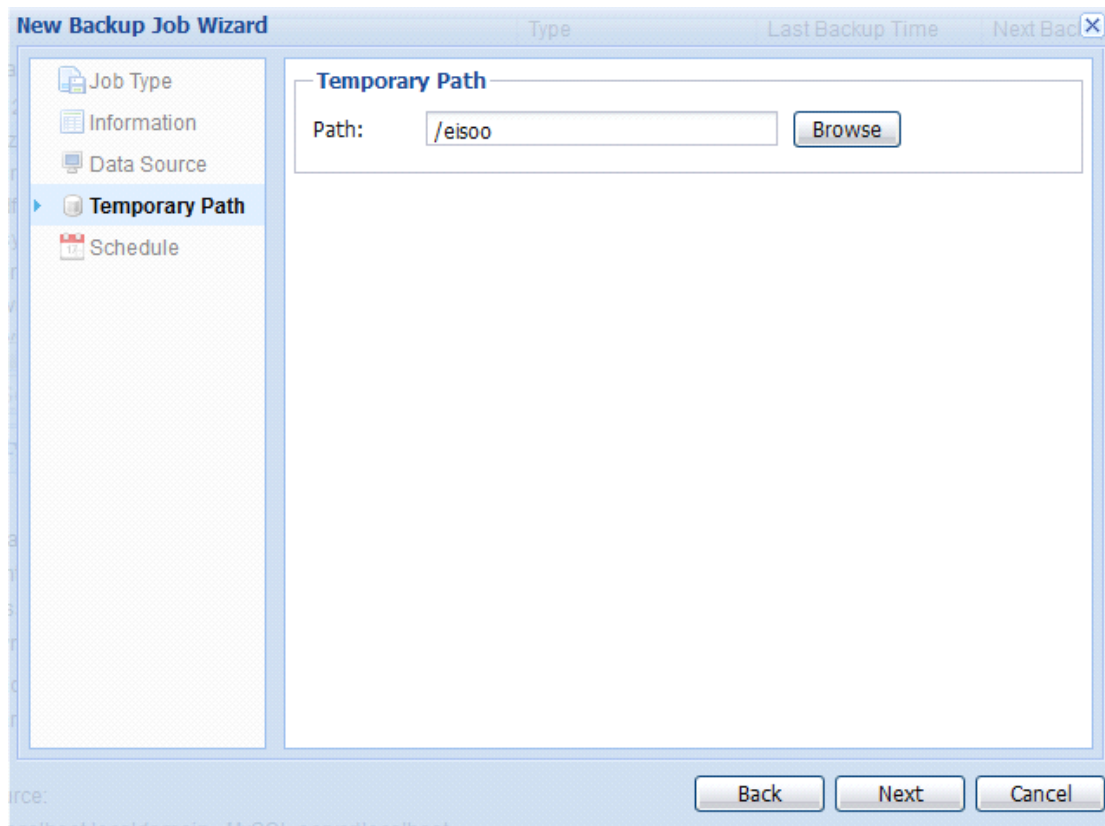
Figure 100　Temporary path of MySQL backup

Step 6: Enter [Schedule/Event] to configure detailed job schedule by using "add, modify, delete". You can also configure media options, compression/encryption and flow control in [Options]. Click [OK] to finish creation.

◆　**Restore Wizard**

Notice for Deployment

1) Preconditions of Restore

If you want to restore the file to a temporary location, there is no need to restore the database. Just ensure there is enough space at the temporary location.

If you want to restore the database, ensure the MySQL service is running and MySQL environment variable is added in path, otherwise script execution will fail, and so will the restore job.

2) Restore Granularity

Restoration of whole server database is supported.

Restore Operation

Step 1: Log in to the Management Console and click "Backup and Restore/Restore" to switch to the browse to restore page.

Step 2: Unfold the backup job to be restored in job list and select the client for restore.

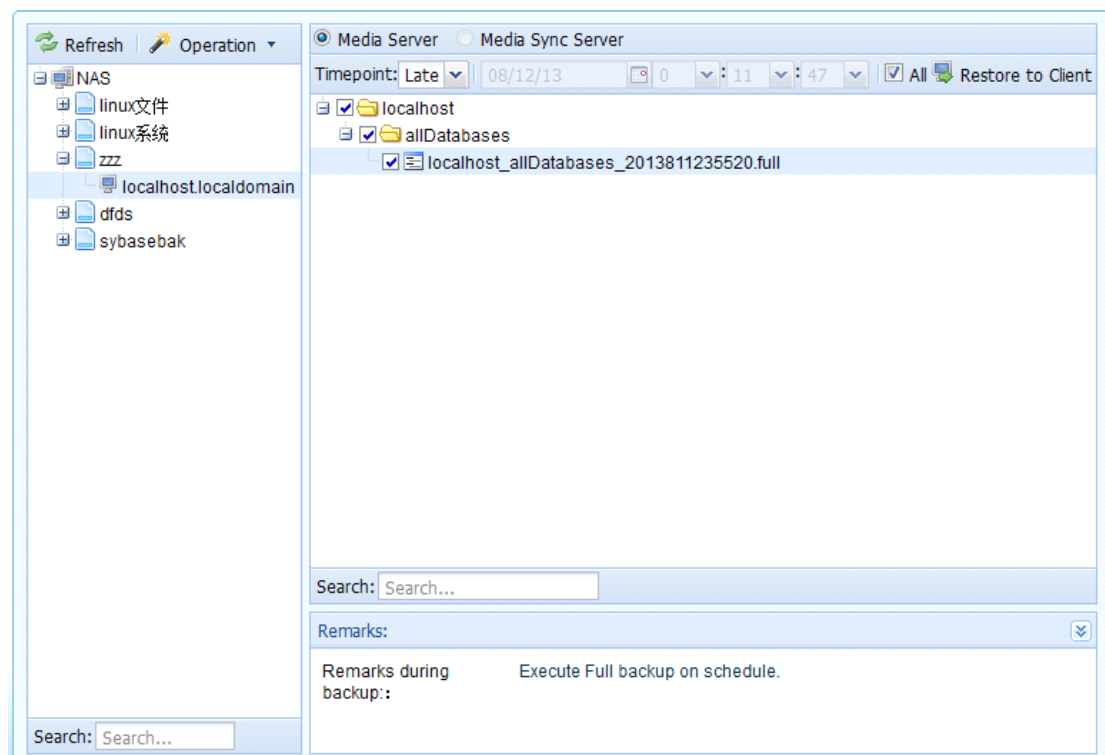Step 3: Click [Time Point] and select one time point.

Figure 101 Select the client to be restored

Step 4: Unfold data source and select the database to be restored. Click [Restore to Client] to show the following:
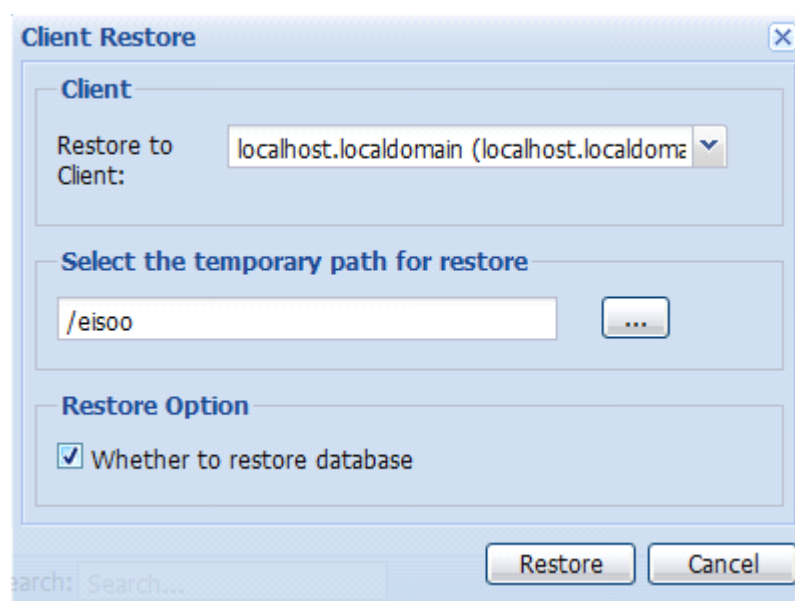

Figure 102 Restore to client

Step 5: Click [Restore] to display the risk warning and click [OK] to submit to execution queue.

6.4.5 Regular Backup and Restore for Virtual Platform

6.4.5.1 Regular Backup and Restore for VMware

◆ **Function Overview**

Backup and restore for VMware of AnyBackup Appliance is based on vStorage which supports VM backup for ESX Server based on shared storage, local storage and iSCSI mount storage. Three backup modes are supported, namely SAN mode, hot-add mode and LAN mode.

◆ **Backup Mode of VMware vStorage**

1. LAN Mode (NBD/NBDSSL Mode)

Whichever storage is used, VMware Storage supports backup in LAN mode under which ESX server reads data from server and then sends it to the machine with the client installed over the network.

nbdssl mode is similar to nbd mode, with similar speed. nbdssl mode adopts encrypted backup, which is suitable for high security backups.

2. Hot-Add Mode

In this mode, we can select one VM on storage to install client to back up other VMs. The storage of VM to be backed up can be accessed by the ESX service of VM with client installed. A special physical server is not required to be client, nor needed to map SAN LUN to VM clients.

In this mode, we can use vStorage to back up any virtual disk files on any storage which can be viewed by ESX server, including NAS and local disk (except for physical RDM compatibility).

Create a snapshot for the VM to be backed up and add a virtual disk file in snapshot (VMDK) to client VM, so as to enable client VM to access to data in virtual disk file. Data is read by the I/O stack of ESX host.

3. SAN Mode

In VMware, if a virtual disk file is stored on FC SAN or iSCSI SAN, you can select SAN mode to back it up. The loading of backups will be transferred to the physical machine with client installed.

◆ **Backup Wizard**

Configure Client

Log in to the system with an admin account and select [System]/[Client] to switch

to the client management interface. Select the client to be configured and click [Configure Virtualization] to show the following:
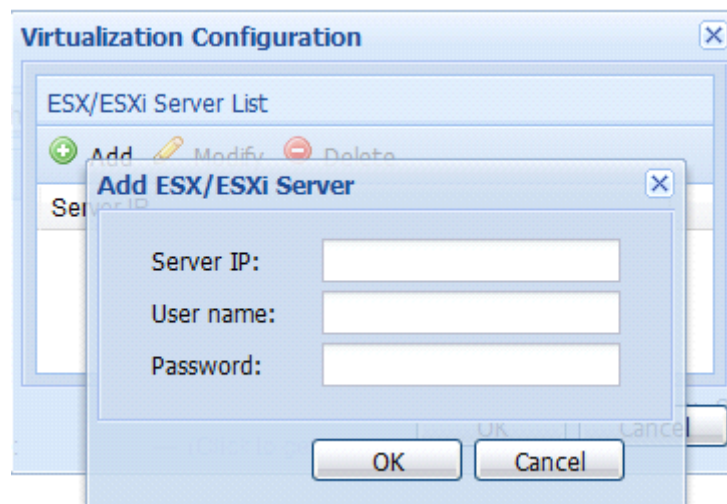

Figure 103 Configure virtualization

Add the IP address, username, password and ensure their accuracy. Otherwise, data source will fail to be unfolded when adding data source.

Click [OK] to finish configuration.

Create Job

Step 1: Enter [Backup] and click [New] to show the [New Backup Job Wizard] dialog. Select [VMware Backup] and click [Next].

Step 2: Enter job name, job group, destination and then click [Next] to continue.

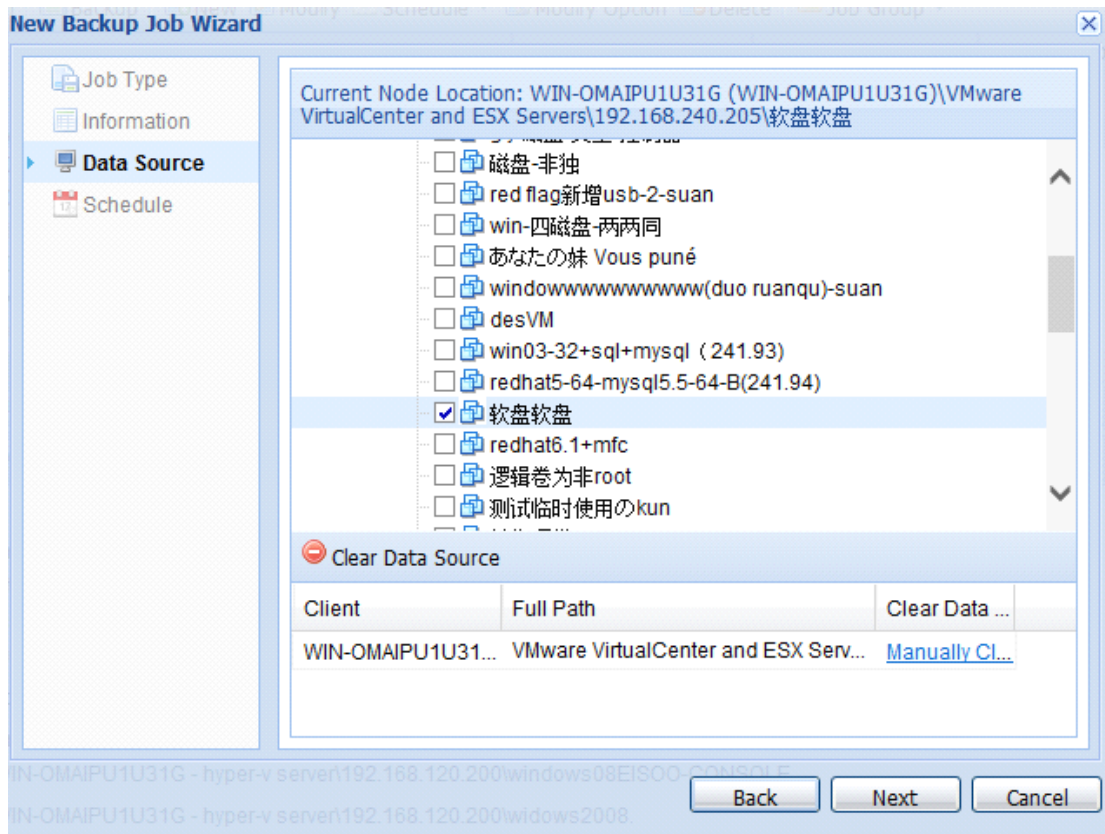Step 3: Enter [Data Source] to select the VM and click [Next].

Figure 104 Select data source

Step 4: Enter [Schedule/Event] to configure detailed job schedule via "add, modify, delete". When configuring the [Start Time], try to choose a time when server is free. Furthermore, when configuring [Retention Strategy], consider your storage space and data demands. Then click [Done] to exit.

Step 5: Configure media option, virtualization and flow control in [Options]. Click [OK] to finish creation.

◆ **Restore Wizard**

Step 1: Log in to the Management Console and click "Backup and Restore/Restore" to switch to the page of browse to restore.

Step 2: Unfold the VM backup job to be restored and select the client for restore.

Step 3: Click [Time Point] and select a time point.

Step 4: Unfold data source to select the VM data to be restored. Click [Restore to Client] to select to restore to existing VM or new VM in "Restore Location". If the former is selected, browse to select the target VM. If the latter is selected, browse to select the storage and resource pool of the new VM.
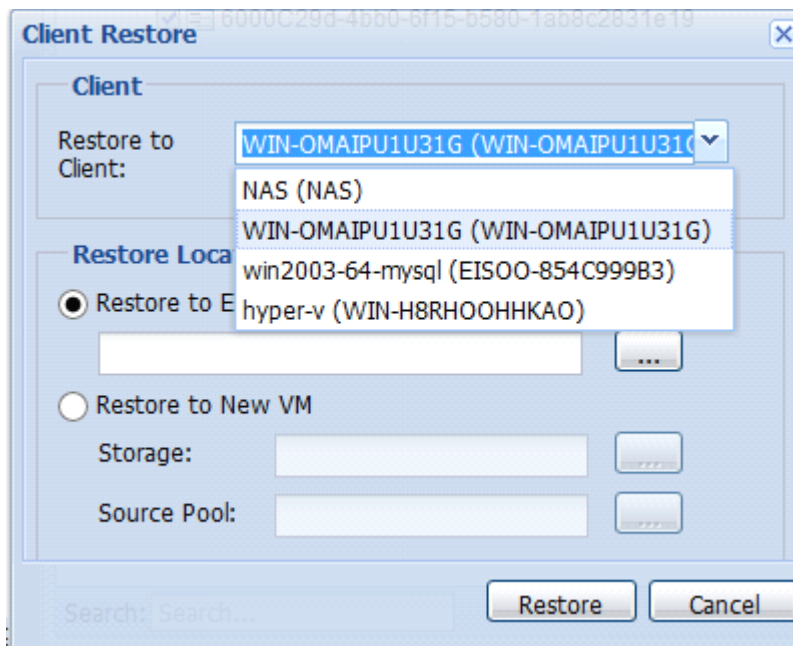
Figure 105 Restore to Client

Step 5: Click [Restore] to show the risk warning and click [OK] to submit to execution queue.

6.4.5.2 Regular Backup and Restore for Hyper-V

◆ **Function Overview**

AnyBackup Appliance supports regular backup and restore for Hyper-V on Windows Server to ensure consistency of time point data, thus ensuring data security of each VM. It supports full backup and incremental backup for VMs. Additionally, it supports restore to original VM or new VM.

◆ **Create Job**

Step 1: Enter [Backup] and click [New] to show the [New Backup Job Wizard] dialog. Select [Hyper-V Backup] and click [Next].

Step 2: Enter job name, job group, destination in [Information] and then click [Next] to continue.

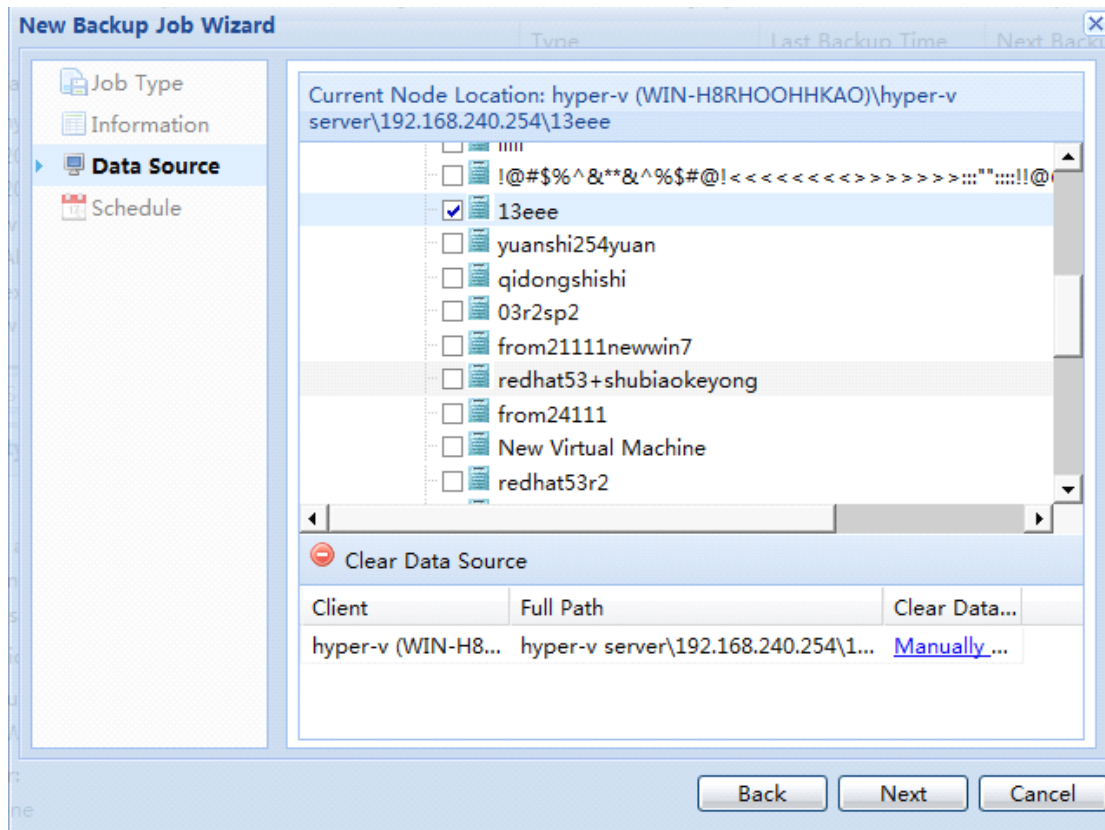Step 3: Enter [Data Source] to unfold the data source to select the VM. Click [Next].

Figure 106 Restore to Client

Step 4 Enter [Schedule/Event] to configure detailed job schedule via "add, modify, delete". When configuring [Start Time], try to back up when the server is free and when configuring [Retention Strategy], consider your storage space and data demands. Click [Done] to exit the wizard.

Step 5: You can also configure media option, compression/encryption, flow control and offline backup in [Options]. Click [OK] to finish creation.
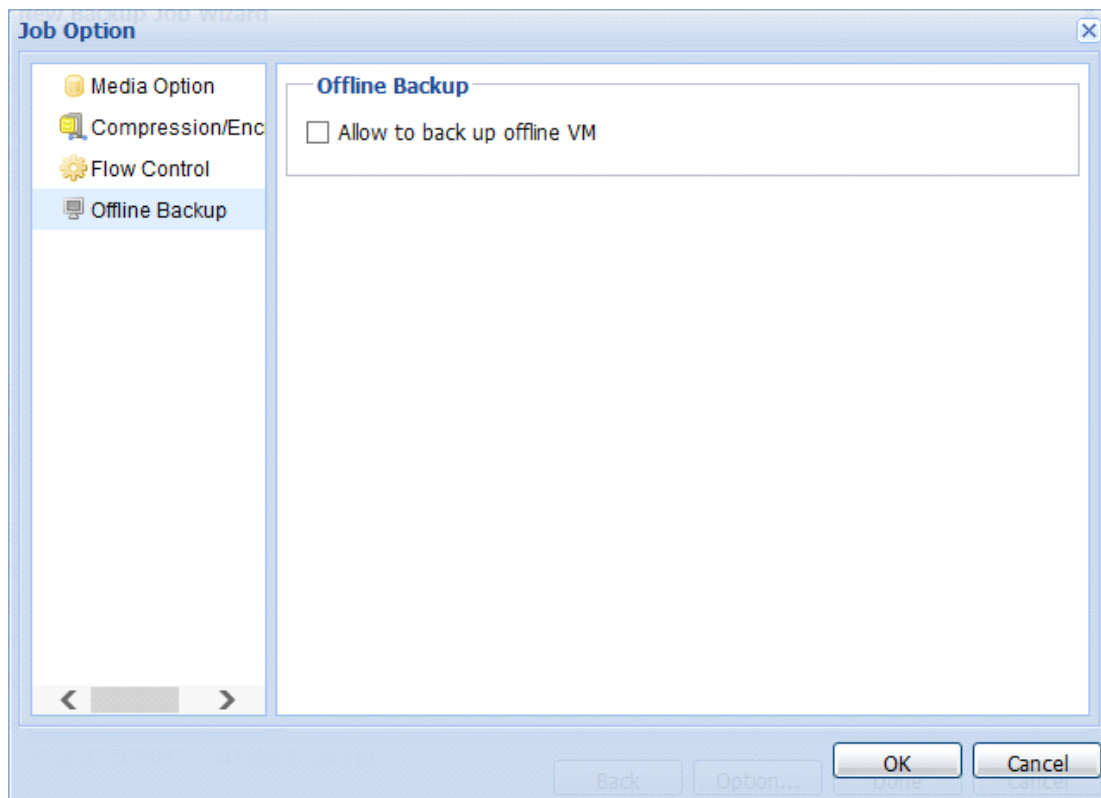
Figure 107 Offline Backup

➢ Mark "Offline Backup" to allow backup for offline VM.

➢ In VM backup, notice will display if the backup job failed.

Step 6: Select Hyper-V backup job and click [Backup]. Select the job type and enter comments. Click [OK].

◆ **Restore Job**

Step 1: Log in to the Management Console and click "Backup and Restore/Restore" to switch to the browse to restore page.

Step 2: Unfold the VM backup job to be restored and select the client for restore.
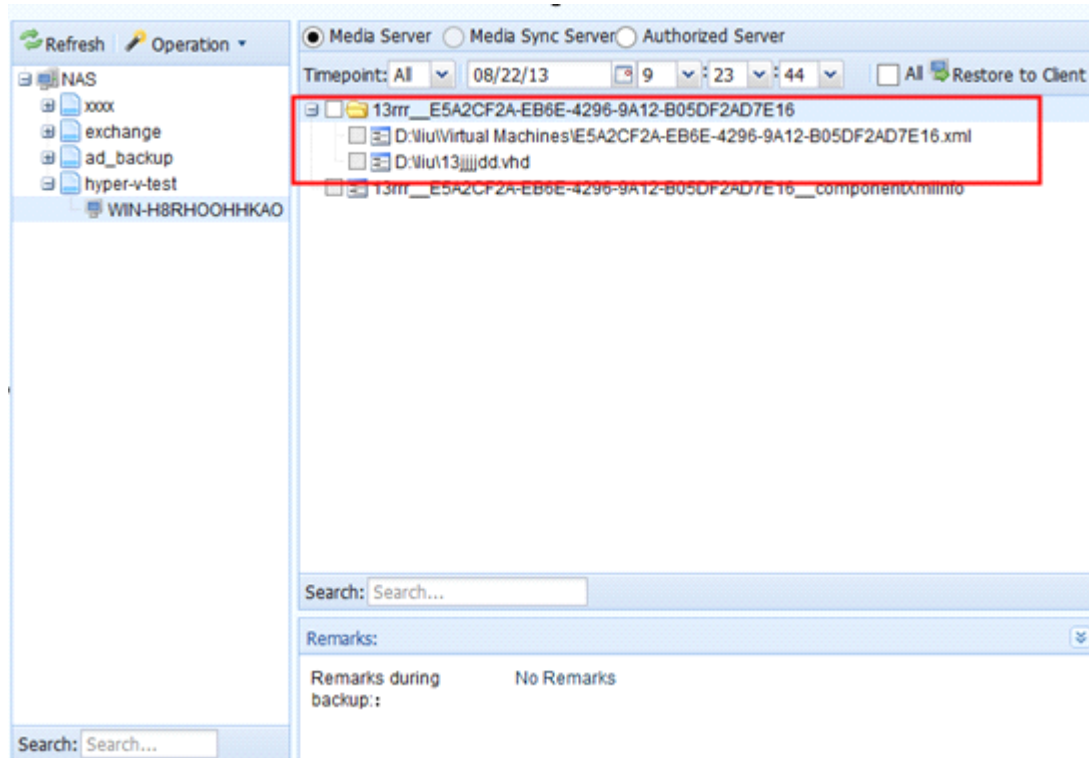
Step 3: Click [Time Point] and select a time point.

Figure 108 Select a timepoint

Step 4: Unfold data source to select the VM data to be restored. Click [Restore to Client] to select to restore to an existing VM or new VM in "Restore Location".
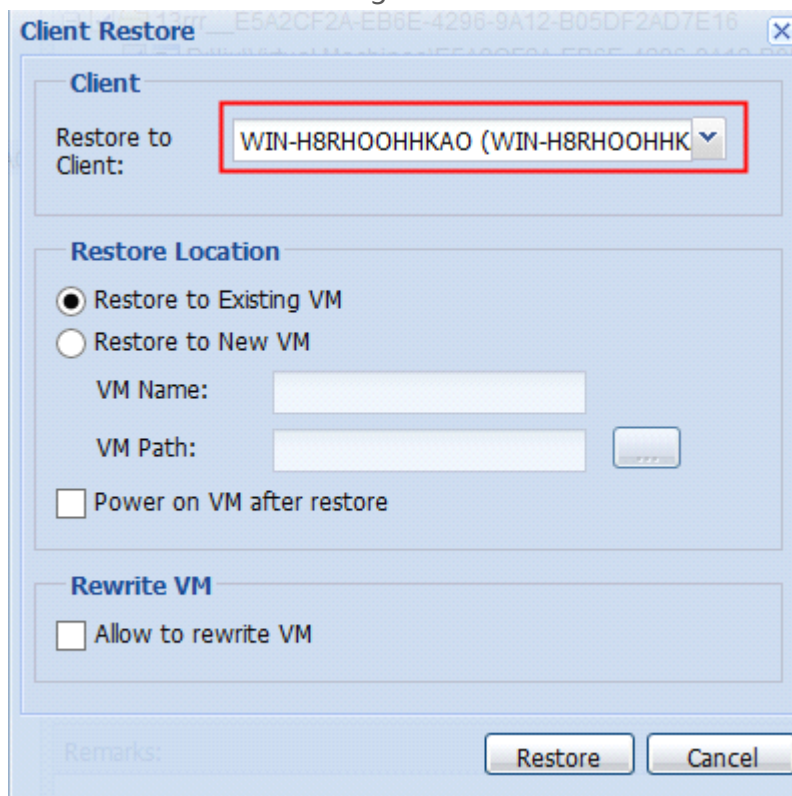

Figure 109 Restore to client

- ➢ If restore to existing VM, rewrite is allowed by default.
- ➢ When restoring to new VM, notice for restore to other locations will show if VM restore of same GUID is performed. Or you can mark 'Rewrite VM' to avoid restore failure.

Chapter 7 Storage Management

7.1 Disk Management

Disk management is the basic function of AnyBackup Appliance. It is achieved by RAID and volume management. Admin can check current disk information by disk management, thus configuring for RAID and volume.

7.1.1 RAID Management

RAID, which is composed of many disks to improve transmission speed and fault tolerance. Click "Storage/Disk/RAID" to enter "RAID management" page, in which RAID can be created, configured and expanded.

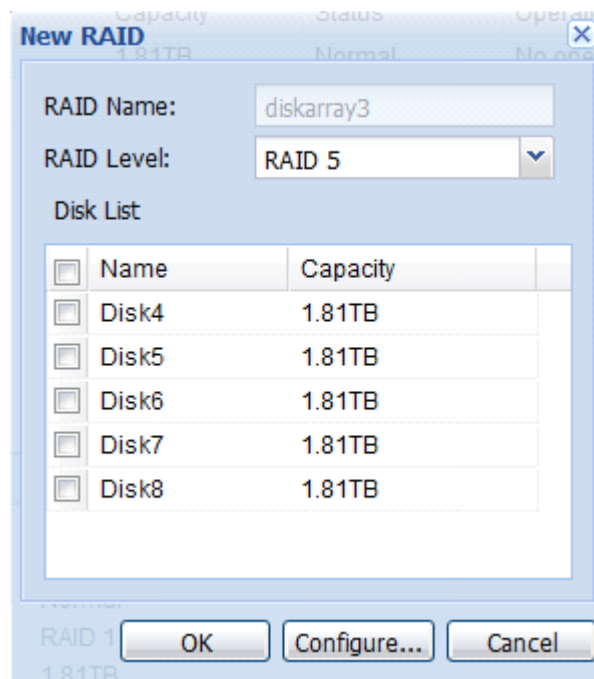Click [New RAID] to open the following dialog box:

Figure 110 Create RAID

➢ RAID Name: used to identify the RAID from diskarray1 to diskarrayN. It is allocated by system automatically.

➢ RAID type: RAID 0/1/10/5/50/6/60. System will automatically list the RAID type available depending on your disk count.

■ If you want to create RAID 0, at least 2 disks are needed;

■ If you want to create RAID 1, at least 2 disks are needed;

- If you want to create RAID 10, at least 4 disks are needed, and total must be even;
- If you want to create RAID 5, at least 3 disks are needed;
- If you want to create RAID 50, at least 6 disks are needed;
- If you want to create RAID 6, at least 4 disks are needed;
- If you want to create RAID 60, at least 8 disks are needed;

➢ Mark the disk to create RAID in "Disk List".

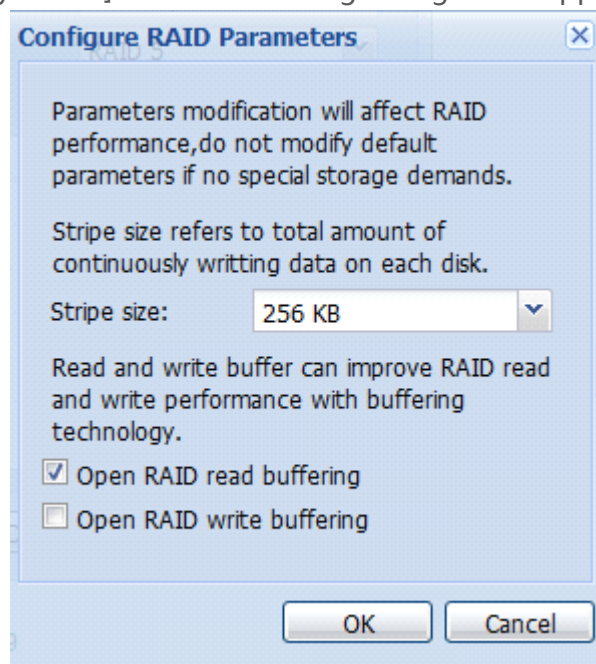➢ Click [Configuration] and the following dialogue will appear:

Figure 111 Configure RAID parameter

- You can configure stripe size and enable read/write buffer. Click [OK] to save configuration or [Cancel] to return without saving changes. Changing the default settings for the RAID is not recommended.

➢ Click [OK] to finish creation.

◆ **Delete RAID**

Select the object and click [Delete].

➢ Click [Yes] to delete the RAID.

➢ Click [No] to return to the previous page.

ᵭ **Note:** Please make sure there is no volume on the RAID to be deleted first.

◆ **Configure RAID**

Used to modify the configuration settings of the RAID. It is similar to the RAID configuration in "Create RAID", but not allowed to modify the script size.

◆ **Rebuild RAID**

➢ When a RAID is in "Degrade", select this RAID and click [Rebuild].

➢ If there is no unused disk, it will display "There is no unused disk, RAID cannot be rebuilt". Click [OK] to return.

➢ Select the unused disk to rebuild RAID, and click [OK] to finish recreation or [Cancel] to return.

◆ **Expand RAID**

➢ Click [Expand RAID] and it will display "There is no disk to expand RAID" if there is no unused disk. Click [OK] to back.

➢ Select the unused disk to expand RAID, and click [OK] to finish expansion or [Cancel] to back.

7.1.2 Volume Management

A volume, also called a logical volume, is logical partition created on a physical disk. Users can access data on partitions.

◆ **Create Volume**

Step 1: click [New Volume] and you will see the following figure:

Figure 112 Create Volume

➢Volume Name: Automatically generated by system and cannot be modified.

➢Volume Type: Backup volume, OFS volume, Shared volume, iSCSI volume, FC volume are included and backup volume is selected by default.

■OFS Volume: for storage of disaster recovery data.

■Shared Volume: for data sharing.

➢Volume Type: Use LVM.

➢Volume Capacity: Enter the volume size and there are three units in the drop-down list: MB, GB and TB, of which GB is default. The value should be a number between 1 and 10000.

Step 2: Select the device for volume creation, click [OK] to finish or [Cancel] to return without saving.

◆ **Delete Volume**

Select the volume to be deleted, and click [OK] to finish or [Cancel] to return.

⌛ **Note:** All data on volume will be lost after volume is deleted. It is recommend that users check before deleting a volume.

7.1.3 Disk List

In "Disk List", you can view all disk information and usage, including disk name, status, physical size, usage and type.

➢ Slot: displays disk slot location of the device.

➢ Status: status of current disk.

  ■ Normal: Disk is working normally.

  ■ Failure: Disk has failed.

  ■ Initialization: Disk is initializing.

  ■ No Disk: No disk has been detected in slot.

➢ Name: named by slot where disk locates, from Disk1 to DiskN.

➢ Volume: Actual volume of disk.

➢ Type: Disk Type.

➢ Usage: Current usage of disk, including initialization progress of disk.

◆ **Refresh**

Click [Refresh] and you can view the latest status of disk.

◆ **Initialize**

Select the disk to be initialized and click [Initialization] to finish initialization.

◆ **New Hot Spare Disk**

Select an unused disk and click [New Hot Spare Disk] to display the following dialog box:
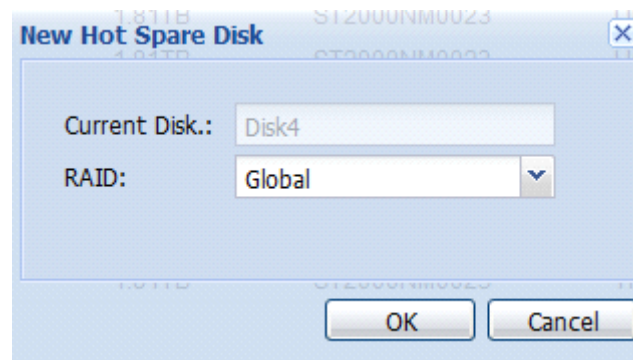

Figure 113 New Hot Spare Disk

Select RAID: Global and all created RAID of level 0, 1, 5. Click [OK] to finish or [Cancel] to back.

◆ **Delete Hot Spare Disk**

Select the hot spare disk to be deleted and click [Delete Hot Spare Disk]. Click [OK] to finish deletion.

➢ Only created hot spare disks will be displayed.

➢ If hot spare disk exists in AnyBackup Appliance, [Delete Hot Spare Disk] can be used. After deletion of hot spare disk, the deleted disk will be free and can be used to create a RAID or Hot Spare Disk.

7.2 Share Management

Share management is used to edit sharing and permission of the directory file which can be used by specified users. It can not only simplify access, but also guarantee the security of data within directories. Continue for an introduction to the introduction of directory, permission, quota and shared service.

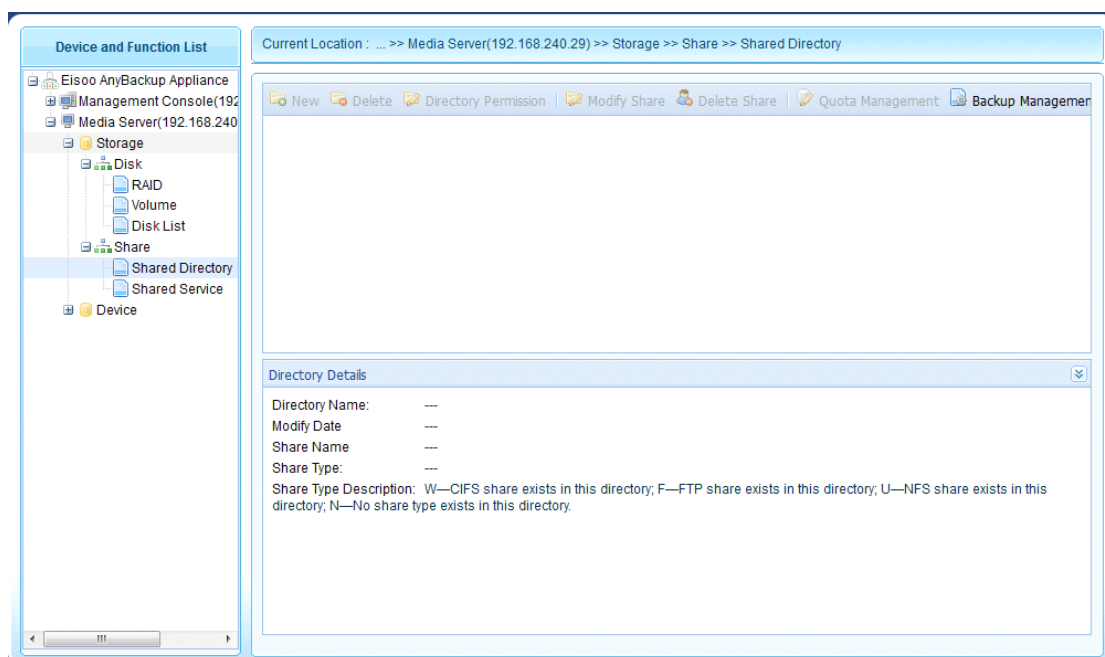Click "Storage/Share Management" and you will see the following:

Figure 114 Share Management

7.2.1 Shared Directory Management

Shared directory management includes share configuration and permission edit of directory file. After share and permission edit, the directory file can contain shared files not allowed to be used simultaneously and shared files allowed to be used simultaneously. By default, multiple users are unable to read or write a file simultaneously.

◆ **Create Directory**

Step 1: Enter "Shared Directory" and select the location to create directory. Click [Create Directory] and the dialog will appear.

Step 2: Enter the new directory name and click [OK] to finish or [Cancel] to return without saving.

> ➢ Directory can be created under volumeX and its subdirectories only. So, before creation, please ensure the volume has been created in the storage device.
> ➢ The directory name can be: letters, numbers, Chinese characters, underscore "_" and hyphens "-" only.

◆ **Delete Directory**

Step 1: Select the directory to be deleted and click [Delete Directory].

Step 2: Click [Yes] on the confirmation window to delete the directory or [Cancel] to back.

ŏ Note: Only directories and subdirectories in shared volume can be deleted.

◆ **Configure Directory Permission**

Step 1: Select the directory to be configured, click [Configure Directory Permission] and mark the check box of "Configure Directory Permission".

Step 2: Configure the permission of user access. Select the user to be configured and click [Read Only], [Read & Write] or [Forbid to Access] to configure his permission. Click [Delete] to cancel the user permission.

> ➢ Special account others: others exist in user list by default. When others is added to permission list, all users and groups except for those already in permission list will execute this operation and change the read & write status. The others account cannot be deleted.
> ➢ If directory is shared, the permission of the shared user (group) depends on the permission of the directory. For example, if the "Configure Directory Permission" of certain user (group) is "Read Only", but "Read & Write" in "Configure Directory Share", the final permission is "Read Only".
> ➢ If there are multi-level directories in a volume and the sub directories are not authorized independently, they will inherit the permissions of parent directory.

Step 3: Click [OK] to finish or [Cancel] to return without saving.

◆ **Configure Share**

After creating a directory, shares need to be configured for multiple users to boast the access permission to this directory. One directory can support share of multiple types simultaneously. There is no relationship between share types so they can be configured independently.

Step 1: Select the directory to be configured and click [Modify Share].

Step 2: Select share type, enter share name, and configure access permission.

➢ Share Name: Self-defined by users, but all the share names must be unique, which means that the newly-created share name cannot be the same as an existing share. If modifying the name of a share, it cannot be the same as other names in the system as well. The share name can only be letters, numbers, and Chinese characters. It cannot contain other characters or spaces, and cannot be "global" or "home" as these are reserved.

➢ Share Type: you can select the following share types:

■ CIFS (Windows): Access to data via CIFS protocol. System will share storage space to Windows clients via CIFS protocol. Users can find the storage device in My Network Places or the client to access to data.

■ FTP (Web): Access to data via FTP protocol. Shared data can be accessed directly from LAN or WAN.

■ NFS (Unix/Linux): If client uses a Linux or Unix system environment, AnyBackup Appliance can set NFS share and data can be accessed by using the mount command of NFS protocol.

➢ Configure Access Permission: Click [Add] to show "Add user/user group permission"

■ If CIFS or FTP share is selected, select the user/user group to be set and click [OK].

■ If NFS share is selected, you can configure host type, allow ROOT or not. If single host is selected, host IP should be entered. Then click [OK].

■ User/User group permission is read only by default. Click "Operation Permission" to select the following permissions: Read only, Read & Write, Ownership.

Step 3: Click [OK] to finish configuration of sharing permissions, or click [Cancel] to return without saving.

◆ **Delete Share**

Step 1: Select the share to be deleted and click [Delete Share].

Step 2: Click [Yes] in the confirmation window to finish deletion or [No] to cancel.

◆ **Quota Management**

Admin can track and control used space on volume quota management. Usable space can be limited by setting a disk quota; warnings will be given if the used space exceeds the warning space.

Quota Space/Limited Disk Space is the max space to be used; Warning Space/Warning Disk Space means the server will give a warning if the used space exceeds the warning space, but the remaining space can be used until it reaches the quota. Warning space should be set close to max space.

For example, if the quota space is set to 500 MB and warning space is set 450 MB, at most 500 MB can be used. When the space used exceeds 450 MB, the system will send a warning. However, the remaining 50 MB of space can still be used.

Quota configuration is for existing users, while default quota is used to configure for new users. If default quota is unlimited, the space allocated is unlimited.

Step 1: Select the volume to be configured and click [Quota]. Click [Default Quota].

When modifying default quota, first select whether to set default limitation for the volume. If you want to limit the quota for the new local users, enter the number and unit in the related space. The unit of disk space is KB, MB and GB, and the numbers should be in the format of common decimal. The numbers can be integer and floating-point number as well, with max length of 8 (including decimal point). Two significant digits will be reserved.

> ➢ Mark "Not limit space to user" and the user will have unlimited space.
> ➢ Mark "Limited space to user" and enter the quota space and warning space, then select KB, MB and GB in the drop-down menu.
> ➢ Click [OK] to finish or [Cancel] to return without saving.

Step 2: Click [Quota] and all current users will be listed.

> ➢ Select one user and click [Configure Quota] to limit disk space for the user.
> ➢ Click [OK] to finish or [Cancel] to return without saving.

Step 3: Switch to "Space Warning" and mark "enable". When the free space of the shared directory is smaller than the warning space, an email will be sent to inform the administrator that the quota is almost being reached.

◆ **Backup Management**

Specific data backup can be performed for each existing volume.

Step 1: Click [Backup Management]

Step 2: Enter required settings in "Backup Server Address" and "Backup Server Port", click "Test Connection" to check whether the address is available.

Step 3: Select the data sharing volume for backup and click [OK] to finish configuration.

7.2.2 Shared Service Management

Using shared service management, you can start a service, stop a service or configure property for executions of various share types. Click "Storage/Share/Share Service".

◆ **Enable Service**

Select the service and click [Start] to start the service.

◆ **Stop Service**

Select the service and click [Stop] to stop the service.

◆ **Configure Service Property**

Select the service and click [Configure Service Property] for related configurations:

- ➢ Configure CIFS Property: Server description can be any character or can be empty, default by server and host name of access object, such as Nas (S116209001); work group is default by workgroup, which can be modified by user.
- ➢ Configure NFS Property: Configure and modify progress count of NFS service, which can be 8, 16, 32, 64 and 128 (default by 8).
- ➢ Configure FTP Property: Five items are included:
  - ■ Port: The default port of FTP is 21 and it must be an integer between 1 and 65535 and cannot conflict with other service ports. If it conflicts with other ports, FTP service will fail to start.
  - ■ Max Clients: The max client count for server to connect simultaneously. It is defaulted by 50 (0 means unlimited clients) and can be set to a whole number larger than 0.
  - ■ Max Client Connections: The connection count for one IP to connect simultaneously. It is 0 by default (0 means unlimited) and can be set to a whole number larger than 0.
  - ■ When "Allow Anonymous User" is not marked, Anonymous users are not allowed to log in to the directory by default.
  - ■ Mark "Allow Anonymous User" and anonymous users can log in to directory by default. You can select the default shared directory name or select in the drop-down list (All shared directories are included.). The selected directory name will be the default login directory and if

there is no shared directory name in the drop-down list, no directory
can be used for anonymous user to log in.

- Click [OK] to finish service property configuration.

Chapter 8 Device Management

With device management, you can configure each device and understand its current status such as energy consumption, network, and more.

8.1 Energy-consumption Management

"Energy-consumption management" is a green and energy-saving technology of AnyBackup Appliance. Click "Media Server/Device/Energy Consumption" and the following dialog box will display:
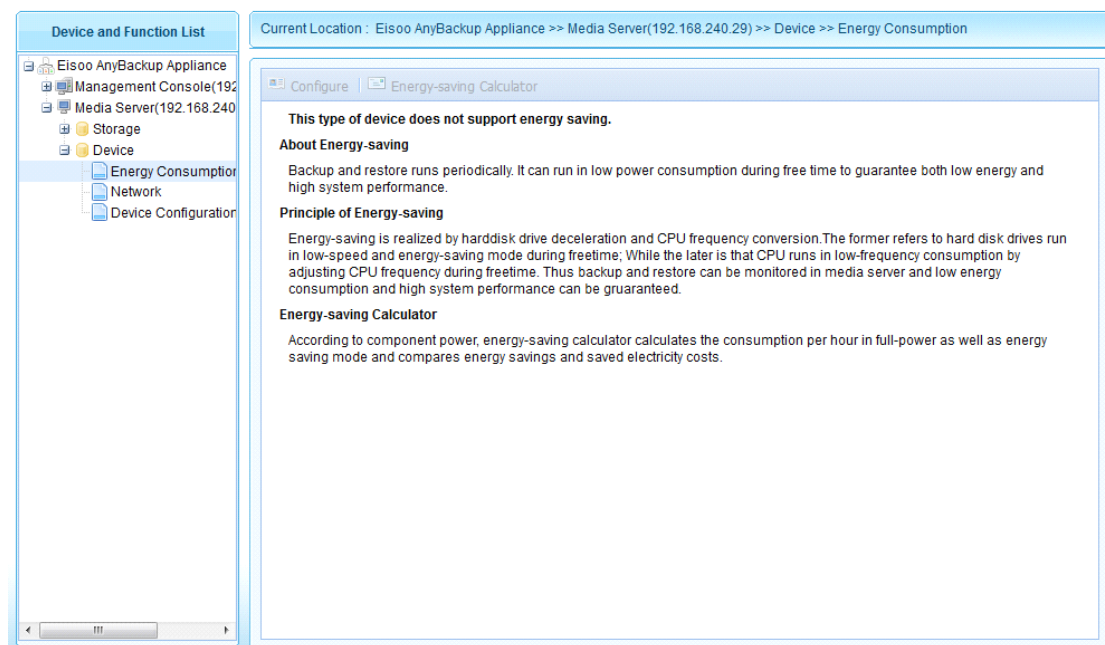
Figure 115 Energy Management

◆ **Configure**

➢ Click [Configure] and mark "Join in green globe plan, Start energy-saving technology", configure time, mark the parts and click [OK] to enable energy-saving technology.

◆ **Energy-saving Calculator**

Energy-saving calculator is to calculate power consumption per hour under full power consumption mode and energy-saving mode according to power of parts, thus summarizing the energy-saving effect and cost saved.

Log in to the management console by using the admin account and click "Media Server/Device/Energy Consumption" then click [Energy-saving Calculator] .

Enter the running time every day, select the parts, enter billing cost and click [Calculate] to generate result.

8.2 Newtork Management

AnyBackup Appliance boasts multiple network interfaces, such as multiple NICs (100M, 1000M). Administrators can configure the IP address of each network interface. It can be assigned automatically by DHCP or BOOTP, or can be configured manually. The following section will introduce network management in detail. Click "Media Service/Device/Network" to display the following:
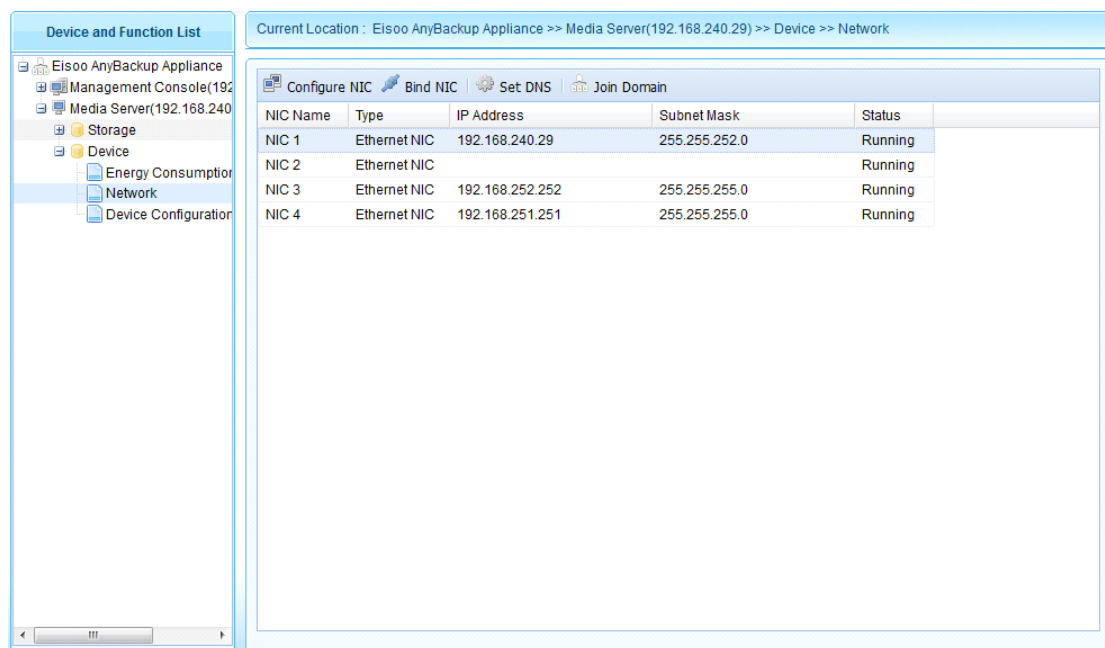
Figure 116 Interface of network management

◆ **Configure NIC**

Each computer needs an IP address. Admin can configure the IP address and network port and how to retrieve it from "NIC Configuration".

Select the NIC and click [Configure NIC] to show the following dialog box:
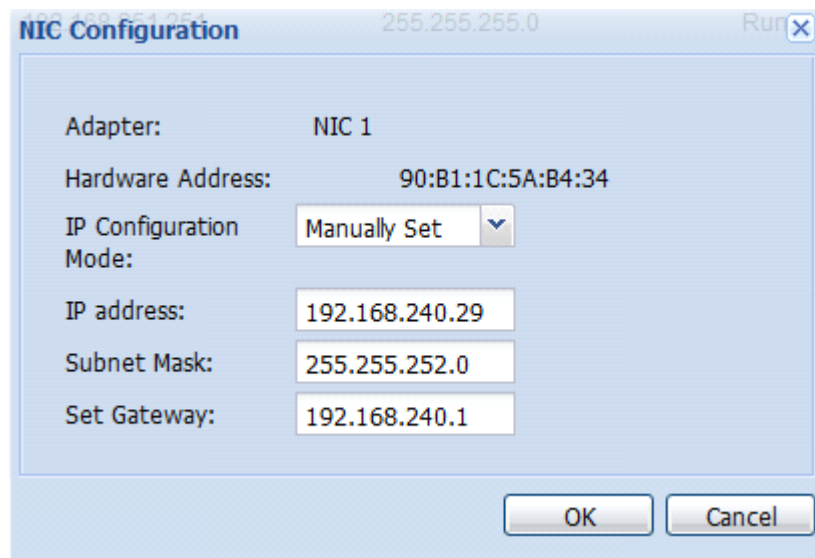
Figure 117 Configure NIC

➢ Select the configuration method of IP (DHCP, BOOTP, manually configure)

- DHCP: obtain IP address automatically through DHCP
- Manually Configure: manually enter the IP address, subnet mask and gateway address.

Click [OK] to finish NIC configuration or [Cancel] to back.

ᴥ Note: After modifying IP address of network port, the browser of client may fail to perform Web management, please change a new IP.

◆ **Bind NIC**

Admin can bind NIC if there are two or more NICs to get higher bandwidth and higher stability.

Click [Bind NIC] and the following dialog will display:
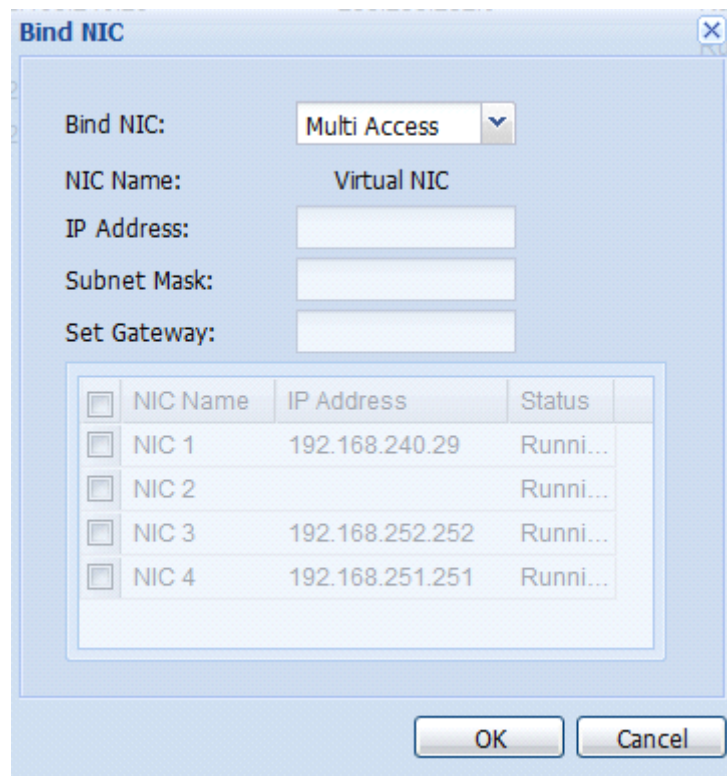
Figure 121 Bind NIC

➢ If "Multiple Access" is selected, users can access to AnyBackup Appliance by using any NIC IP. Click [OK] to finish configuration or [Cancel] to return without saving.

➢ If "Load Balancing" or "Fault Redundancy" is selected, users need to enter valid IP and network mask and mark the bound NIC. Then click [OK] to finish configuration or [Cancel] to return (The count of bound NIC cannot be less than 2).

■ Load Balancing: the bound NICs will allocate the average data flow. When one fails, its flow will be transferred to other NICs.

■ Fault Redundancy: NICs can be redundant. If there is one working NIC currently, other NICs will replace it automatically when this NIC fails.

■ Multiple Access: Work independently from each NIC, being in different segment.

◆ **Configure DNS**

➢ Click [Configure DNS].

➢ Enter preferred DNS and alternate DNS. When preferred DNS failed, the alternate DNS will automatically take over the job of preferred DNS.

➢ Click [OK] to finish the configuration of DNS or [Cancel] to back.

◆ **Join Domain**

Click [Join Domain] and the following figure will display:

Figure 118 Join Domain

➢ Host name can be modified (host name is the server label displayed in Windows network neighborhood). It can be letters, numbers, and underscores. But it must start with a letter. After modification, start Windows (CIFS) service and it will take effect.

➢ Mark "Workgroup" and click [OK] to finish configuration or [Cancel] to return without saving.

➢ Mark "Domain" and enter domain name, host name, domain controller IP, domain admin and password. Click [OK] to finish configuration or [Cancel] to return without saving.

 Note: Domain name must be upper-case while host name of domain controller must be lower-case.

8.3 Device Configuration

Using device configuration, you can view AnyBackup Appliance info and modify host name. Click "Media Server/Device Management/Device Configuration" to show the following dialog:
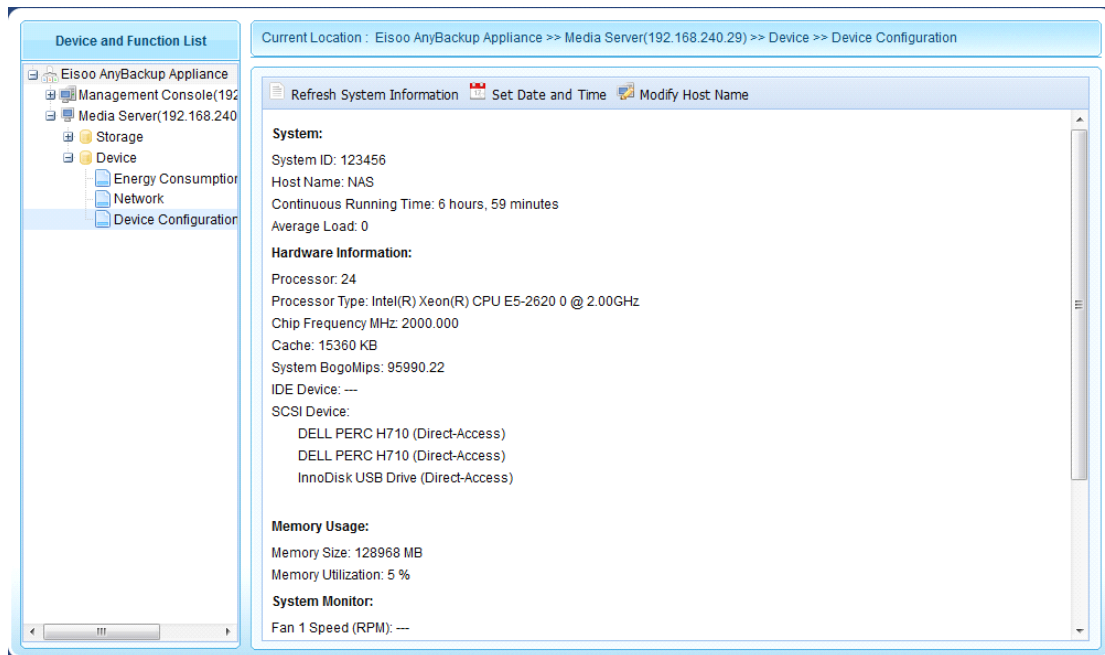
Figure 119 Device configuration

◆ **Refresh System Information**

Click [Refresh] to view the latest status of device system, which includes:

➢ System: Including serial number, host name, continuous running time and average loading statistics.

➢ Hardware Info: Including processor count, type, frequency, cache capacity and more.

➢ Memory Used: System memory size, used percentage.

➢ Battery Info: Display whether battery protection is enabled. If not, it will display that the battery is not installed. If yes, detailed battery status will be displayed, which includes battery temperature, remaining energy, remaining time.

➢ System Monitor: CPU voltage, temperature, fan speed and more.

➢ Date and Time: Display the current date of time.

◆ **Configure Date and Time**

Click [Configure Date and Time] and the following dialog will be shown:
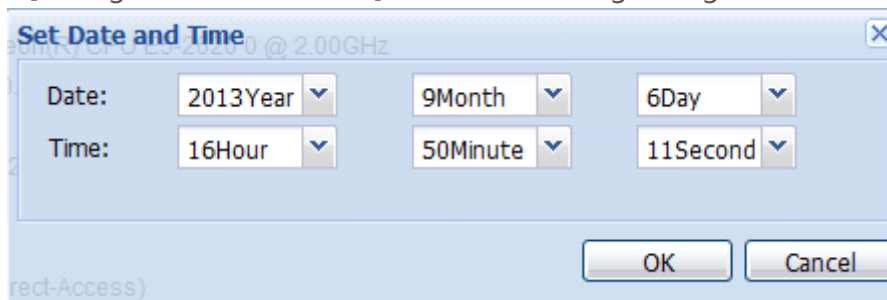
Figure 120 Configure Date and Time

➢ Click the drop-down menu of date column to select the required year, month and day.

- ➢ Click the drop-down menu of time column to set the time.
- ➢ Click [OK] to finish time configuration or [No] to return without saving.

◆ **Modify Host Name**

Click [Modify Host Name] to display the following dialog:
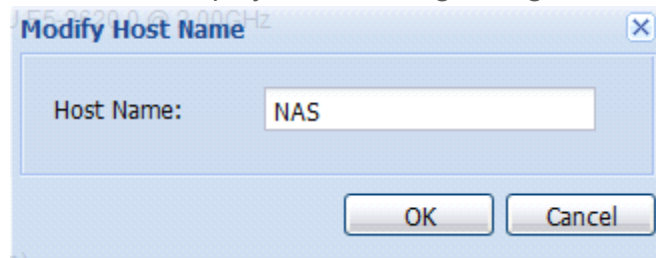
Figure 121 Modify host name

- ➢ Enter new host name in "Host Name", which should be composed of letters and numbers, and it must start by letters.
- ➢ Click [OK] to save modification or [Cancel] to return without saving.

ᕍ Note: The host name should be composed of letters and numbers, and must start with a letter.

Chapter 9 Report Management

9.1 Home

Report management contains Basic Information, Recent Risk, Risk Statistics and Business Status.
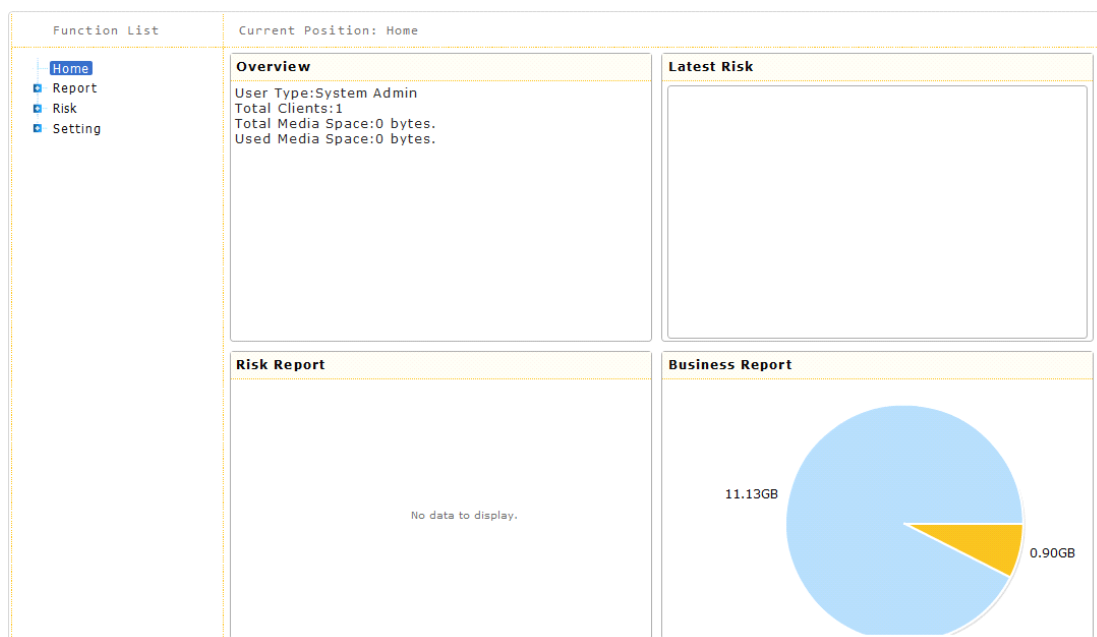
Figure 122 Home--system user

- ➢ Basic Information displays user type, total client count, total media space and used media space.
- ➢ Recent risk displays the latest 6 records after risk. Click [View Details] to skip to the risk monitor interface of Risk Management to handle risks.
- ➢ Risk statistics displays the number of risks of different types.
- ➢ Business status report displays business data of various types, including file, operating system, email and database.

9.2 Navigation Line

Click the navigation line on the top right corner to enter the different sections.
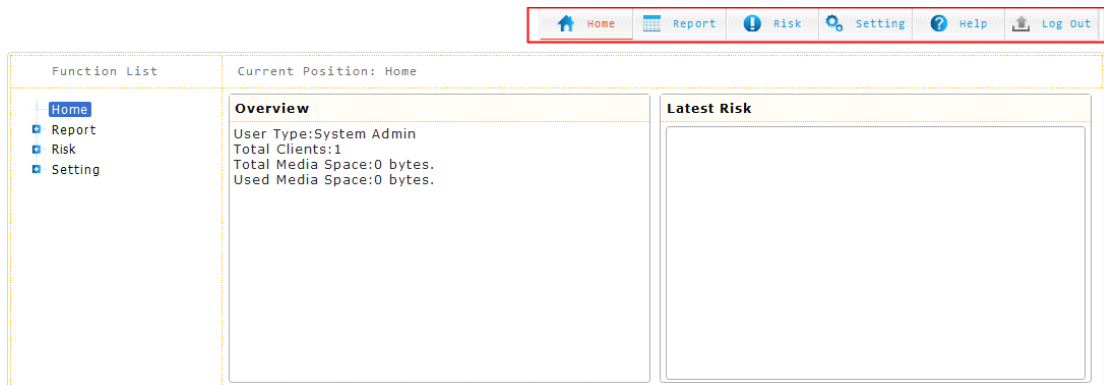
Figure 123 navigation line

➢ Report statistics links to "Report Statistics/Console".

➢ Risk management links to "Risk Management/Risk Monitor".

➢ Configuration links to "Configure/Role".

➢ "Help" links to help document of Report Management Center.

➢ Click Exit to return to the console.

9.3 Report Statistics

9.3.1 Overview

Report is the most direct reflection of enterprise management objects. In report statistics, users can view the required data information.

9.3.2 Console

Click "Report statistics/Console" and the security status report can be viewed along with capacity status reports and business status reports shown as follows:
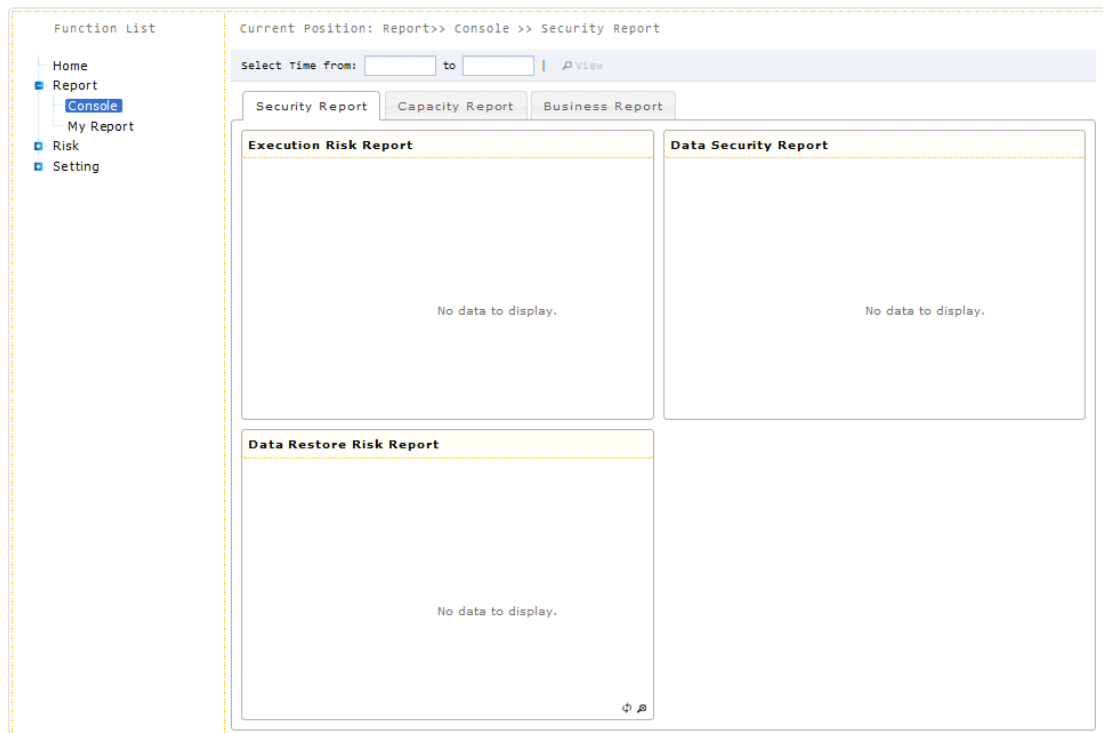
Figure 124 Security status report of console
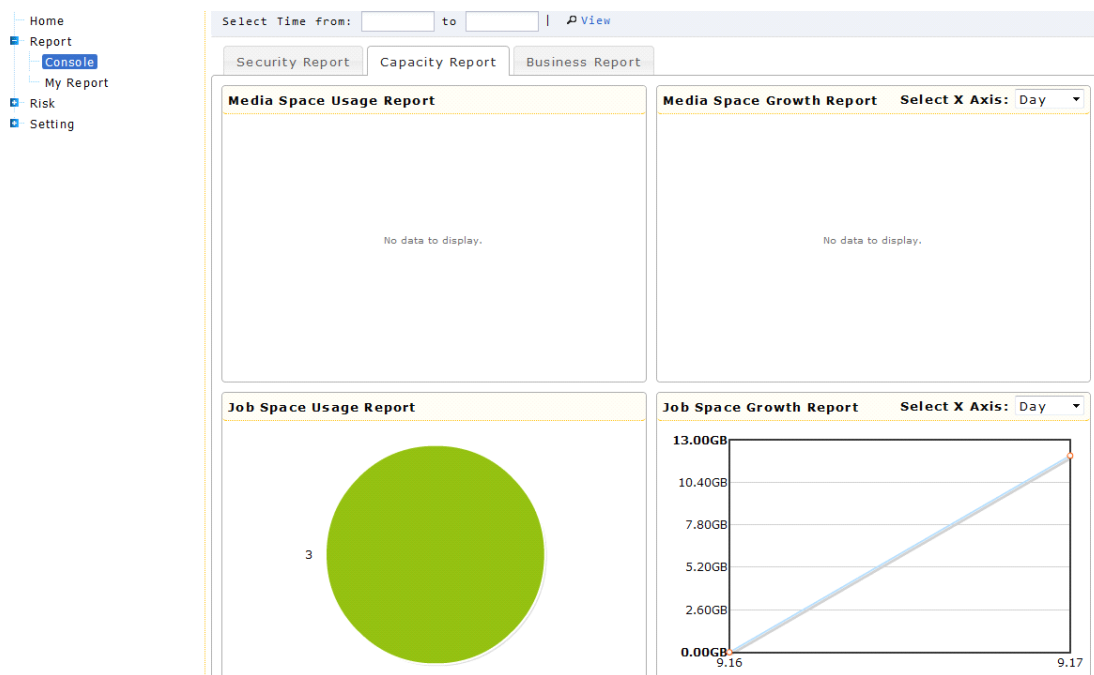
Figure 125 Capacity status report of Console
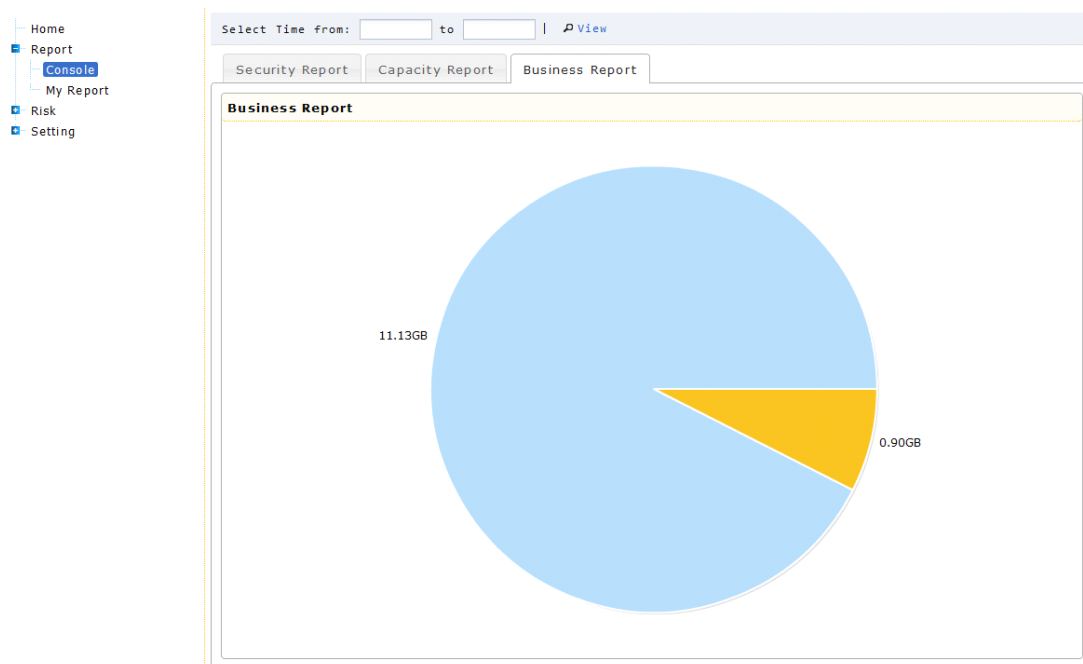
Figure 126 Business status report of Console

➢ The start time displays the creation date of system center by default, while the end time displays the current date.

➢ Select the time period wanted and click [View] to view report. Reports of all time periods can be viewed.

5.3.3 My Report

To display a customized report, users can configure a custom report type, report shortcut in My Report. The main interface is as follows:
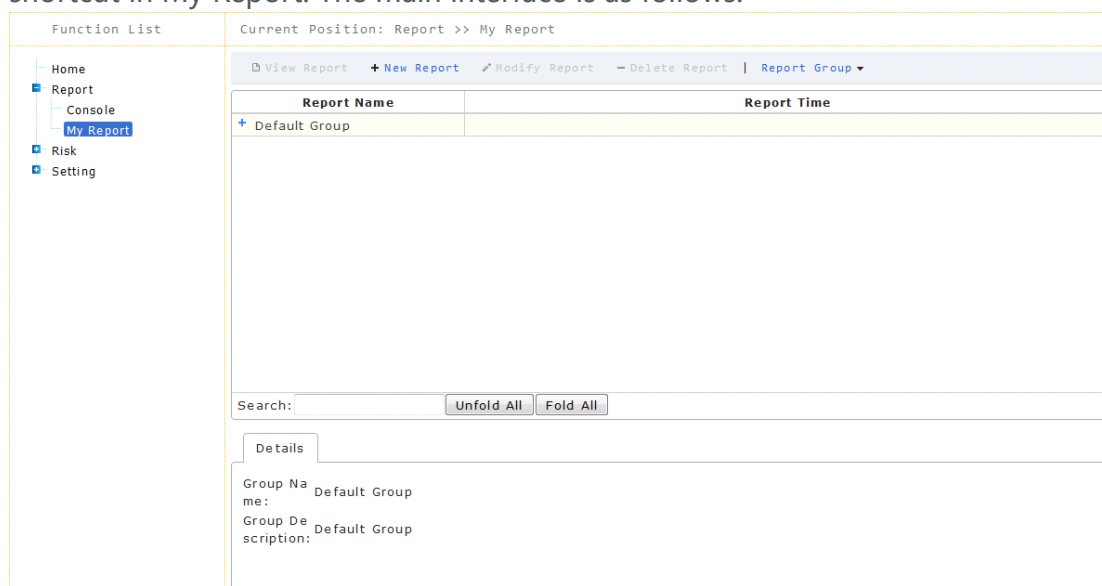
Figure 127 My Report

➢ Enter the My Report page, and the first report is selected by default.

- ➢ Click report and its detailed information can be viewed on the left bottom.
- ➢ Select one job and click [View] to view all information of the job.
- ➢ Select one job and click [New] to show the new report wizard.
- ➢ Select one job and click [Modify] to show the modify report wizard.
- ➢ Select one job and click [delete] to show the confirmation window. Click [Yes] to delete, or [No] to cancel.
- ➢ Click [Report Group Management] to create, modify and delete report group.

◆ Create Report

Click [My Report]/[New] to show the new report wizard which is shown as follows:

Figure 128 Create Job

Basic Info

- ➢ Enter report name and description in Basic Info. If it is invalid, click [Next] to display " The report name should be between 3-50 characters, and ~`!@#$&%,.;: cannot be included. "
- ➢ Select the report group drop-down menu to view all report groups created. Users can select the report group as required.
- ➢ Report description can be empty, and its length should be less than or equal to 200 characters. If not, it will display "The report description exceeds 200 characters".

Select Report

- ➢ Security status report displays:
  - ■ Execution Risk Report
  - ■ Data Security Risk Report
  - ■ Data Restore Risk Report

- Capacity status report displays:
  - Media space usage report
  - Media space growth report
  - Job space usage report
  - Job space growth report

Time Type

- There are three time types: fixed time (by default), duration time and repetition time.
- Fixed time refers to the time period when report is fixed. The start time and end time are absolute, such as from July 1th, 2013 to Aug 10th, 2013.
- Duration time means the time period of report changes with the current time, such as from July 1th, 2013 to now.
- Repetition time means the period of report is periodical, such as 10th to 20th every month.

◆ **Modify Report**

Click [Modify] to display the following dialog box"

Figure 129 Modify Report

- Basic information, time type can be modified.

◆ **View Report**

Select one report and click [View] to view detailed information.

◆ **Delete Report**

Select the report to be deleted and click [Delete] to display the following dialog box:

Report Name	Report Time
− Default Group	
myreport	2013-9-17 ~ 2013-9-18

Delete Report ✖

All the reports in the group to delete will be moved to default group, are you sure to delete selected report group?

OK Cancel

Search:

Details
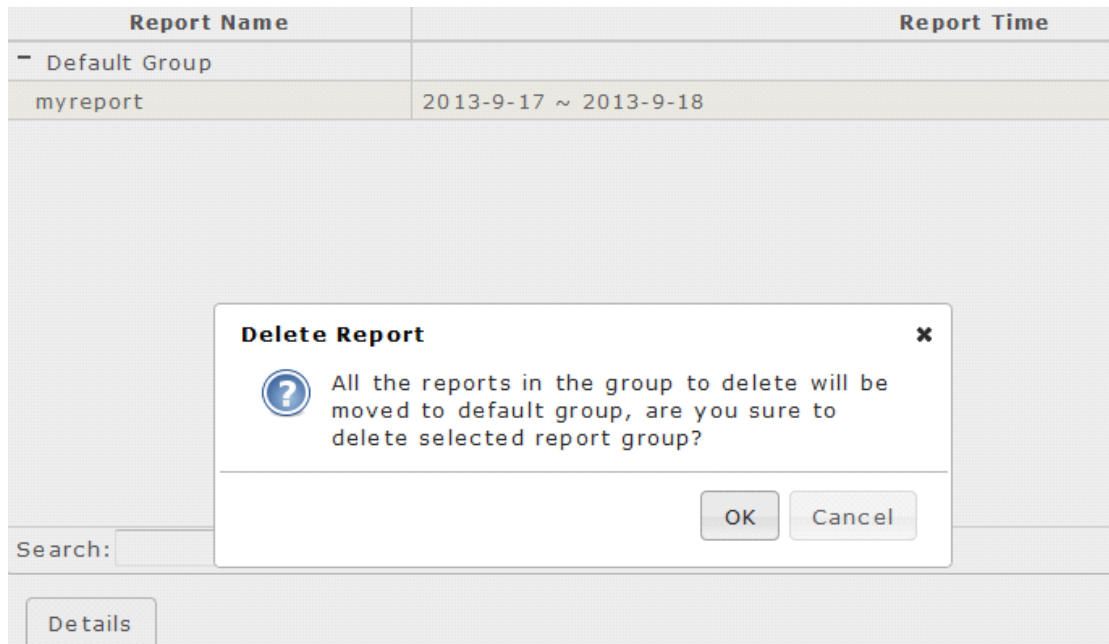
Figure 130 Delete report

➢ Click [OK] on the confirmation window to delete the report, or click [Cancel] to cancel deletion.

◆ **Report Group Management**

New Group

Click [Report Group]/[New] to display the following dialog box:

Figure 131 Create report group

- ➢ Member list displays the tree structure of Group-Members.
- ➢ The length of group name should be between 3 and 50 characters, and ~`!@#$&%,;: cannot be contained.
- ➢ The length of group description should be less than 200 characters.
- ➢ Group names cannot be the same. If there is an existing group with the same name, an error will be shown, "Groups of same name are not allowed, please re-enter".

Modify Report Group

Click [Report Group]/[Modify] to show the following dialog box:

Figure 132 Modify report group

Delete Report Group

Click [Report Group]/[Delete Group] to show the following dialog box:

Figure 133 Delete report group

➢ Click [OK] to finish deletion or [Cancel] to cancel deletion.

9.4 Risk Management

9.4.1 Overview

In risk management, you can view risk level, configure system risk, monitor risk, view risk management record, etc.

9.4.2 Definition for Risk

Risk includes execution risk, data security risk and data restore risk.

Execution Risk

Execution risk primarily displays the execution risk and its risk level. Risk level cannot be modified. Click [Execution Risk] and you can see the following interface:
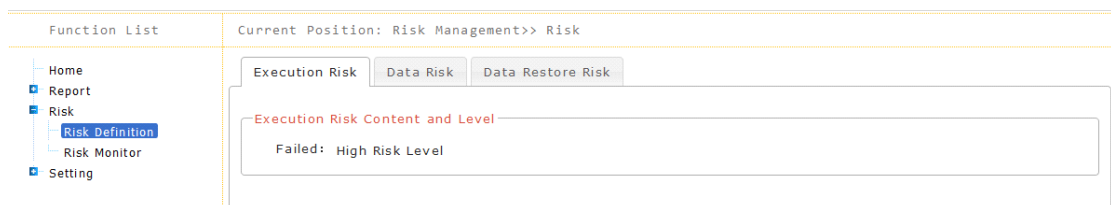
Figure 134 Execution Risk

Data Security Risk

Data security risk mainly displays the data security risk and its risk level. Click [Data Security Risk] and you can see the following interface:
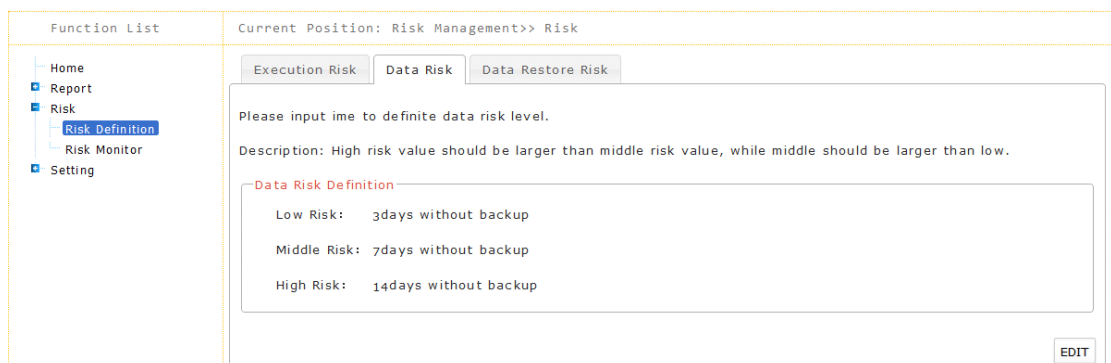
Figure 135 Data Security Risk

➢ Default system risks and risk levels:
- High risk: no backup for 14 days
- Middle risk: no backup for 7 days
- Low risk: no backup for 3 days

➢ The risk level can be defined by entering days in the textbox.

➢ The days entered must be positive integer between 1 and 999. Otherwise, an error will display.

Data Restore Risk

Data restore risk displays data restore risk and its level. Click [Data Restore Risk] and you can see the following interface ;

Figure 136 Data Restore Risk

➢ Default data restore risk and risk level

■ High Level (%): the value of theoretical restore time minus RPO is over 200% times than RPO

■ Middle Level (%): the value of theoretical restore time minus RPO is over 100% times than RPO

■ Low Level (%): the value of theoretical restore time minus RPO is over 50% times than RPO

➢ The percentage and network bandwidth of each risk level can be configured according to environment.

➢ The percentage entered must be a positive integer between 1 and 999, otherwise notice will display.

➢ The network bandwidth entered must be positive integer between 1 and 999999, otherwise notice will display.

➢ The RPO entered must be positive integer between 1 and 999, otherwise notice will display.

9.4.3 Risk Monitor

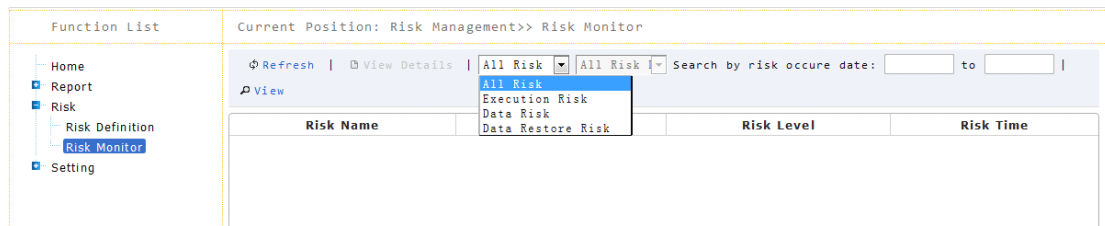Click "Risk Management/Risk Monitor" to enter the interface as follows ;

Figure 137 Risk Monitor

➢ Select a risk and click [View Details] and information of risk name, type, source, level, time and suggestion will be displayed.

9.5 Configuration

9.5.1 Overview

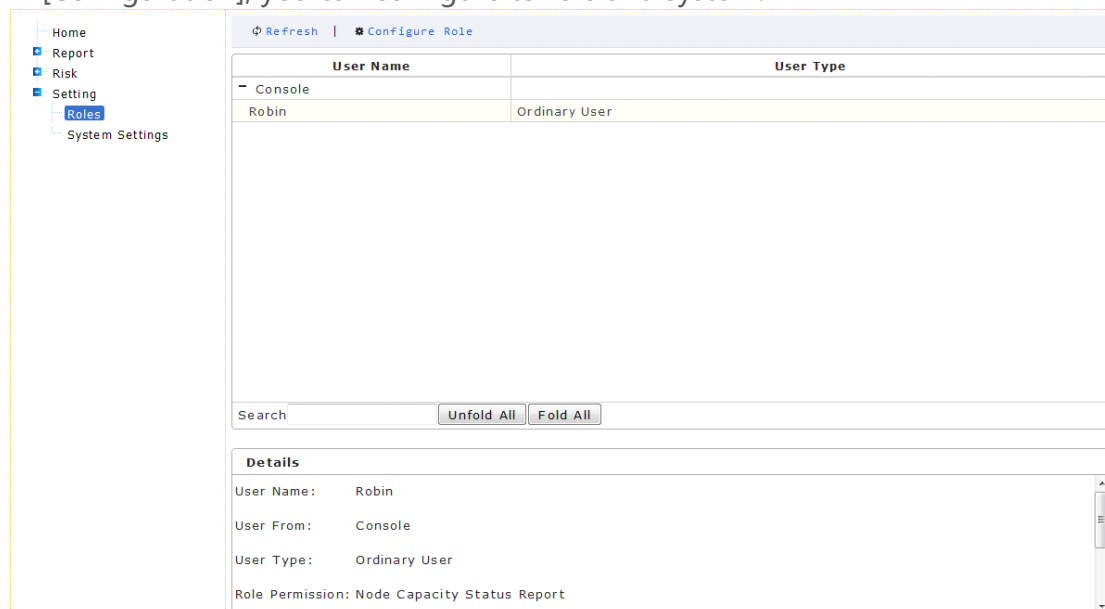In [Configuration], you can configure to role and system.

Figure 138 Role Configuration

9.5.2 Role Management
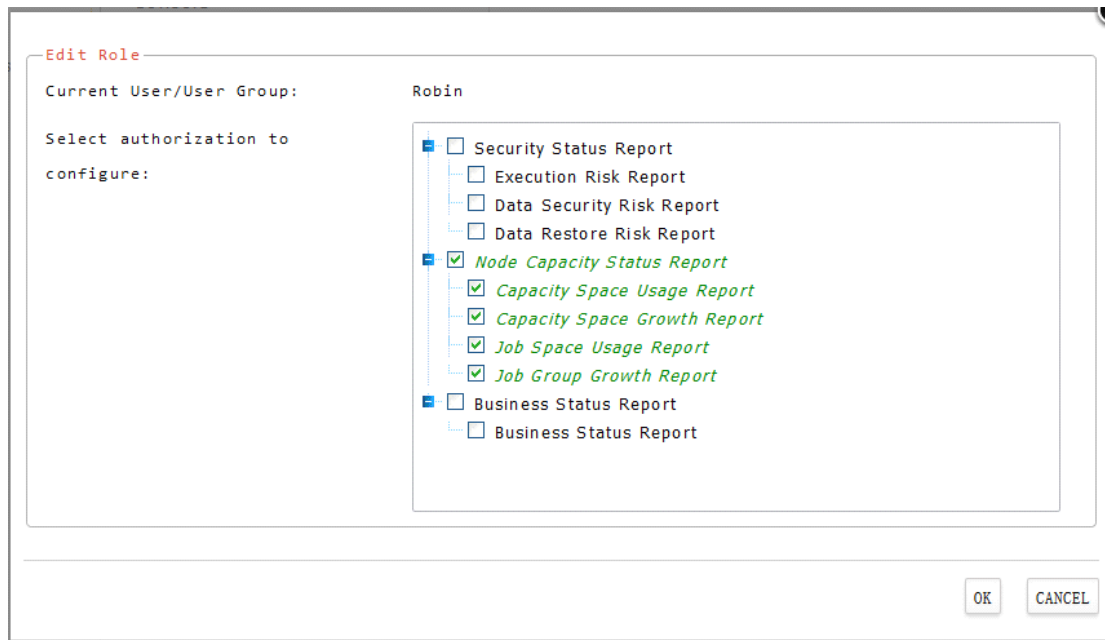
Click [Role Configuration] to show the following:

Figure 139 Edit Role

Permission includes:

- ➢ Security Status Report
  - ■ Execution Risk Report
  - ■ Data Security Risk Report
  - ■ Data Restore Risk Report
- ➢ Capacity Status Report
  - ■ Capacity Space Usage Report
  - ■ Capacity Space Growth Report
  - ■ Job Space Usage Space
  - ■ Job Space Growth Report
- ➢ Business Status Report
  - ■ Business Status Report

9.5.3 System Configuration

In [System Configuration], you can configure risk notification, which means whether to notify system administrator of console or system center to handle risk by email.

Figure 140 Risk notification

➢ Click [Edit] and the above options can be configured.

Click [Resume Default Configuration] and all default values will be displayed. Click [Save] to resume default configuration or [Cancel] to cancel.

AnySupport

AnySupport is a new type of service product provided by EISOO to satisfy user requirements for data backup and restore. Based on enterprise data, EISOO AnySupport not only responds in 24 hours, but also plays the role of [Data Health Management Consultant] and [Exclusive Technical Expert].

The service tenet of AnySupport is professional, excellent and active. In other words, we plan data management programs for customers actively, examine customer data periodically, and help customers to build an effective backup system with professional and excellent service. AnySupport contains technical support service, professional service and training certification service.

Furthermore, EISOO provides free phone support for our customers and partners. If you have any technical problem or doubts about our product, please feel free to contact us:

◆ Domestically Free Technical Hotline：   400-880-1569

◆ Global Hotline: 086-21-54222601

◆ Quality Supervision Hotline: 021-54326440-8201

◆ Technical Support Email：   support@eisoo.com

Address: No.1188 Lianhang Rd, Minhang District, Shanghai, China

Tel: +86-21-54222601

Skype: eisoo-overseas

Email: support@eisoo.com